Get To Grips
With
Data Protection

South Somerset District Council
Training Session For Members

11th June 2015
Get to Grips With Data Protection

Gill Smith
DP Assist

Data Protection Act - What's It All About?

- Safeguard rights and freedoms of individuals
- 8 legally enforceable principles
- Enforced by the Information Commissioner - Christopher Graham

New EU Data Protection Regulations

- Individual’s rights strengthened - Right to be forgotten/erasure
- No charge for access to your own information or notification (registration)
- More reliance on consent and justification for collecting, using, disclosing information
- Notify breaches of principle – mandatory
- Privacy by design – built into systems
- Enforcement action against service providers (data processors)
### Enforcement

#### Offences
- Unauthorised obtaining or disclosure of personal data (Section 55)
- Procurement – to acquire, sell or offer to sell information unlawfully
- Non-compliance - Enforcement or Information Notice
- Non-Notification and failure to notify changes to your Register Entry
- Forcing someone to make a subject access request to check their criminal past (Section 56)

#### Penalties
- Serious breach of principle – monetary penalty up to £500,000
- Offences – Now unlimited fine if Magistrates' Courts

### Which Hat Are You Wearing?

- For the Council eg serving on a committee?
- For your constituents?
- For your political party?
- Personal, domestic, recreational purposes?

### Whose Information is Covered?

- Living identifiable individuals (of any age)
- Not de-personalised or statistical information
- Not businesses or organisations
- Not the deceased
Personal Data
- Makes a person identifiable from information that you have or could obtain about them
- Relates to them - helps you to learn, record, or decide something about them
- They are the focus
- Should be of biographical significance

Sensitive Personal Data
- Racial or ethnic origin
- Political opinions
- Religious or other beliefs
- Trade Union membership
- Physical or mental health or condition
- Commission or alleged commission of an offence
- Any offence proceedings their disposal or sentence of any court.

More Definitions
- Data Subject – person who the information is about
- Processing – obtaining, using, storing, destroying etc
- Data Controller - controls manner and purpose(s) of processing
- Data Processor - processes on behalf of data controller
- Third Party - Anyone except data subjects, employees, or agents of data controller

Principle 1 – Fair Processing
Provide a Privacy Policy, Privacy Statement or Fair Processing Notice:
- Data subjects should be informed of:
  - Identity of who they provide it to or nominated representative if you are not based in the UK
  - Purpose(s)
  - Anything else to make it fair. For example who you share information with
- Exemptions may apply:
  - Crime prevention/detection/apprehension
  - Taxation
  - Required by law to disclose
  - Disproportionate effort if you receive it from a third party
Principle 1 - Lawfulness

- Must not contravene other laws such as:
  - Human Rights Act – Article 8
    - Right to respect for private and family life.
    - (Privacy Impact Assessments)
  - Common Law Duty of Confidentiality
    - Overrides:
      - Consent
      - Legal requirement or obligation
      - Crime prevention/apprehension or prosecution of offenders
      - Risk of harm to person or someone else
      - Public interest

Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011

- Applies to sending advertising materials (including newsletters, event information etc) – by text, email, fax.
- Includes unsolicited (including automated) phone calls to business and private individuals – check the Preference Service at www.tpsonline.org.uk
- Use of Internet Cookies on websites - small file of letters and numbers downloaded on to a device when websites accessed.
- Consent required
- Enforced by the Information Commissioner

Principle 2 – Secondary Use and Notification

Must not be used in any way that is incompatible (or clashes with) its ORIGINAL purpose

Assess:
- Change of use? Seek consent?
- Disclosures to third parties?

Example - Social Media Use: Create a specific Councillor account or page to keep personal and political use separate. You can then share information with constituents and colleagues without disclosing personal information about yourself, friends and family.
**Notification**

Public register at www.ico.gov.uk
- £35 fee – annual renewal
- Must be kept accurate and up to date
- You must amend it within 28 days of changes such as new purpose(s)
- Criminal offence not to be registered or updated.

Exemptions include:
- Core business purposes
- No information held on computer

**Principle 3, 4 and 5 – Good Information Management**

- Adequate relevant and not excessive
- Accurate and kept up to date
- Not held longer than necessary

Review, Retain, Destroy or Archive

**Principle 6 Individual’s Rights**

Subject Access
- What are individuals entitled to?
- What makes a valid request?
- What Are Your Responsibilities When Responding To and Dealing With a Request?
- Optional:
**Principle 6 Individual's Rights**

- Have personal data corrected or deleted if inaccurate or misleading (via courts)
- Prevent processing likely to cause damage or distress
- Object to direct marketing
- Object to automated decision making
- Compensation
- Request an assessment

**Principle 7 - Take Appropriate Security Measures**

**Conduct A Security Risk Assessment:**

- Whose information is it?
- What personal data are held, how and where?
- Vulnerabilities and threats?
- Nature of harm/distress caused to them if unauthorised or unlawful access/loss/damage/theft/disclosure
- Consequences to your organisation?
- What technology is available and at what cost?
**Principle 7 - Take Appropriate Security Measures**

- Must ensure: Confidentiality, Integrity, Availability
- Control Access: Secure passwords (change default ones), safe storage and transit, protect from others, secure destruction
- Protect Your Information Systems
  - Secure, long, difficult to guess passwords, changed regularly
  - Anti-Virus, malicious software and hacking protection
  - Secure networks (including WiFi - Wireless)
  - Removable Media - Encryption eg memory sticks
  - Keep software upgrades up to date

**Using Your Own Device**

- What work information is stored on it? – Keep it separate from private use
- Where is it stored? (memory card, cloud) – Keep it secure (encryption, trusted providers)
- What apps are installed or downloaded? Obtain from trusted providers
- Who has access to it? – Keep it away from others
- How is it secured? Strong password, locks if not used, pin number, encrypted, up to date anti-virus protection, latest security upgrades installed?
- What is it connected to? Beware public networks – do not automatically connect.
- What happens if it is lost or stolen? Can it be wiped securely?

**Principle 7 - Take Appropriate Security Measures**

- Protect from fire, flood, and accidental damage - Sales and off-site storage of backups (test them), disaster recovery plans
- Organisational measures - ensure employee reliability
  - Policies, procedures, training, vetting, keep informed
  - "Data Protection and Information Security Key Points for Councillors"
  - "ICT Guidelines for SSDC Councillors"
- Service Providers (Data Processors)
  - Must have written contracts
  - Act only under your instructions
  - Ask for security guarantees and action to be taken
  - Right of audit/inspection/compliance monitoring
Principle 8 - Overseas Transfers

OK to send information overseas if:

- Country or territory is within the European Economic Area
- Or adequate protections in place
  - “Safe” or Third Countries eg Canada
  - Safe Harbor – USA companies or organisations

If not, then
- Must satisfy Schedule 4 Conditions eg seek consent, can transfer if to protect vital interests, public register, contract in place etc

BEWARE - includes internet and social media use

Dealing with Disclosures

- Was individual informed about it? Reasonable expectation?
- Lawful? Condition for processing satisfied? Duty of confidentiality?
- Is disclosure required by law? (Section 35) eg Member powers to inspect documents necessary for your work
- In connection with legal proceedings, seeking legal advice or establishing, exercising or defending legal rights? (Section 35)
- For prevention and detection of crime or taxation? Overriding public interest? (Section 29)
- Emergency? Matter of life or death?

- Freedom of Information or Environmental Information request?
Data Protection Principles

(Schedule 1 of the Data Protection Act)
The Data Protection Principles

1. Personal data shall be processed fairly and lawfully, and, in particular, shall not be processed unless
   ■ At least one of the conditions in Schedule 2 is met; and
   ■ in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4. Personal data shall be accurate, and, where necessary, kept up to date.

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6. Personal data shall be processed in accordance with the rights of data subjects under this Act.

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss, or destruction of, or damage to, personal data.

8. Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Definition of Processing – extract from the Information Commissioner’s Legal Guidance:

“Processing, in relation to information or data, means obtaining, recording or holding the information or data (which includes, in relation to personal data, obtaining or recording the information to be contained in the data) or carrying out any operation or set of operations on the information or data, including –

- organisation, adaptation or alteration of the information or data;
- retrieval, consultation or use of the information or data (which, in relation to personal data, includes using the information contained in the data);
- disclosure of the information or data (which, in relation to personal data, includes disclosing the information contained in the data) by transmission, dissemination or otherwise making available, or
- alignment, combination, blocking, erasure or destruction of the information or data.”
Conditions for Processing

(Schedules 2 and 3)

and

Sensitive Data
# Data Protection Act Conditions for Processing

The Data Protection Act requires that you may **not** process **personal data** unless you can satisfy **at least one** of the conditions in Schedule 2 of the Act, which are summarised below:

## Conditions for Processing Personal Data (Schedule 2 of the Data Protection Act)

<table>
<thead>
<tr>
<th>Data subject has given their consent</th>
<th>Processing is <strong>necessary</strong>:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>For the exercise of any functions of the Crown, a Minister of the Crown or a government department.</td>
</tr>
<tr>
<td></td>
<td>For any other functions of a public nature exercised in the public interest.</td>
</tr>
<tr>
<td></td>
<td>For the legitimate interests of the data controller or those of a third party to whom the data may be disclosed.</td>
</tr>
<tr>
<td></td>
<td>This is information needed to carry out the work and business of the data controller provided it does <strong>not</strong> prejudice the rights and freedoms or legitimate interests of the data subject. (For example if a person fails to pay money owed to your organisation, their name and address information may be disclosed to a debt recovery organisation to recover the money).</td>
</tr>
</tbody>
</table>

If the information is sensitive data you must **also** meet at least one of the conditions in Schedule 3

## Conditions for Processing Sensitive Personal Data (Schedule 3)

<table>
<thead>
<tr>
<th>Individual has given their <strong>explicit</strong> consent</th>
<th>The processing is <strong>necessary</strong>:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>For the exercise of any statutory functions carried out by the data controller, required by or under law.</td>
</tr>
<tr>
<td></td>
<td>For medical purposes undertaken by a health professional or someone who owes a duty of confidentiality equivalent to that of a health professional.</td>
</tr>
<tr>
<td></td>
<td>Racial or ethnic origin information that is only collected to monitor or review equality of opportunity or treatment, and with safeguards for the rights and freedoms of individuals.</td>
</tr>
</tbody>
</table>

© Copyright DP Assist 2014
Sensitive data are:

- the racial or ethnic origin of an individual,
- their political opinions,
- their religious beliefs or other beliefs of a similar nature,
- whether they are a member of a trade union,
- their physical or mental health or condition,
- their sexual life,
- the commission or alleged commission by them of any offence, or
- any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings.

There are also certain circumstances that occur by Statutory Instrument where sensitive data may be processed without having to obtain explicit consent. Briefly, these are:

- Equal opportunities and fair treatment - identifying or keeping under review the existence or absence of equality of opportunity or treatment relating to their beliefs and physical or mental health
- Confidential counselling, advice, support or any other services in the substantial public interest
- Prevention or detection of any unlawful act in the substantial public interest
- Discharge of any function designed to protect members of the public against dishonesty, malpractice or other seriously improper conduct etc in the substantial public interest
- For journalistic, artistic or literary purposes
- Insurance or occupational pension schemes
- Political opinions held by registered political parties
- Research purposes in the substantial public interest
- Processing carried out by Police Constables
- Disclosures of sensitive data to elected representatives
- Processing of criminal offences and payment card information relating to indecent photographs of children.
- Disclosure of prisoners’ release information to Members of Parliament
- Disclosure of sensitive data to the Hillsborough Independent Panel relating to the Hillsborough Stadium Disaster.