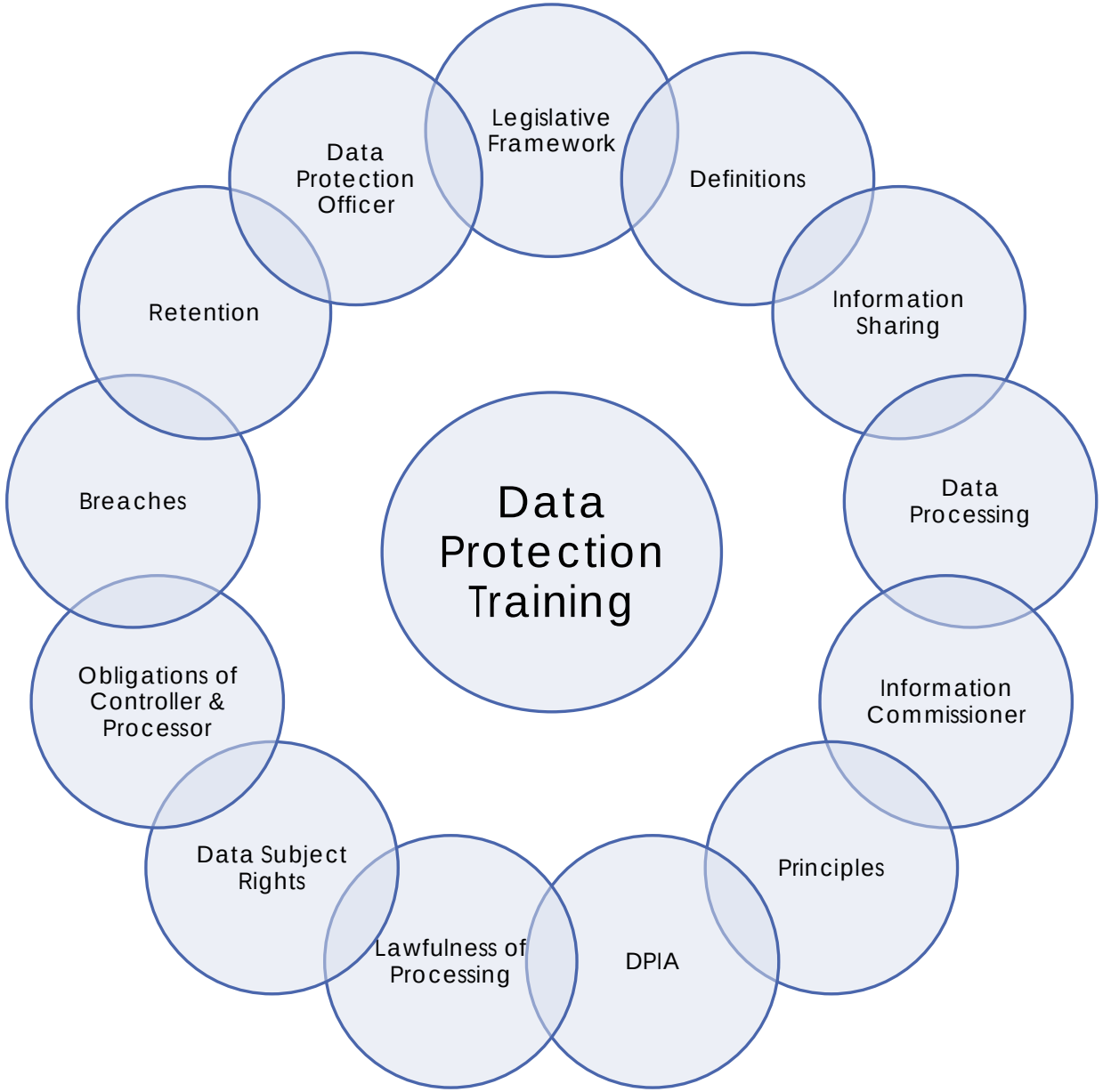
Police & Crime Commissioner
West Yorkshire

Data Protection Training

Level 1 & 2

Topics


Data Protection Training
Legislative Framework
Definitions
Information Sharing
Data Processing
Information Commissioner
Principles
DPIA
Lawfulness of Processing
Data Subject Rights
Obligations of Controller & Processor
Breaches
Retention
Data Protection Officer

Part 1

WY – OPCC
Data Protection Training
Jan, 2019

Security of Processing

Personal data must be processed securely by means of 'appropriate technical and organizational' measures.

- Considers risk analysis
- Considers Organizational Policies
- Considers Physical and Technical Measures
- Consider state of art and cost of implementation
- Appropriate to circumstances and risk of processing
- Use pseudonymisation and encryption where appropriate
- Able to restore access and availability in a timely manner
- Able to test effectiveness of measures and undertake improvements

What was considered good and best practice under DPA 1998 is now a legal requirement.

Information Security Policy

Good Practice

Top of Mind:

- Use strong passwords.
- Screen lock your device when not in use.
- Do not use unauthorised USB or mobile devices.
- Be vigilant concerning unknown websites, links or attachments.
- Secure important documents. Clear desk policy.
- Beware of ‘social engineers’ who may use social media to gain your confidence or access to sensitive information.

Information Security Policy

Good Practice

Top of Mind:

- When using mobile devices in public, beware of ‘shoulder surfers’ who can peer over your shoulder to view and gain access to confidential information.
- Don’t leave digital assets where a thief can easily steal them.
- Don’t use your personal mobile device for business purposes unless authorised to do so.
- Don’t connect work related devices to unknown or untrusted networks e.g public WI-FI hotspots.
- When working agile, ensure that no other person has access to official and confidential information.

Protective Markings

Historic Classification

- Government Protective Marking Scheme (2014)

- **Not Protectively Marked**: The information is unclassified or a protective marking is not required.
- **Protect**: Information can cause distress to individuals, financial loss, improper gain, prejudice investigations, facilitate crime or disadvantage government policy.
- **Restricted**: The release of the information will have effects such as significant distress to individuals, adversely affecting the effectiveness of military operations, or to compromise law enforcement.

Protective Markings

Historic Classification

- Government Protective Marking Scheme (2014)

- **Confidential**: Releasing this level of information can cause such effects ; considerable infringement on personal liberties, material damage to diplomatic relations, or to seriously disrupt day-to-day life.
- **Secret**: Release of this information can cause side-effects that may be life-threatening, disruptive to public order or detrimental to diplomatic relations.
- **Top Secret**: Release of the information can cause considerable loss of life, international incidents or severely impact ongoing intelligence operations.

Protective Markings

New Classification

- Government Security Classification (2018) – 4 Principles

1. ALL information that HMG needs to collect, store, process, generate or share to deliver services and conduct government business has intrinsic value and requires an appropriate degree of protection.

2. EVERYONE who works with government (including staff, contractors and service providers) has a duty of confidentiality and a responsibility to safeguard any HMG information or data that they access, irrespective of whether it is marked or not, and must be provided with appropriate training.

Protective Markings

New Classification

- Government Security Classification (2018) – 4 Principles

3. Access to sensitive information must ONLY be granted on the basis of a genuine 'need to know' and an appropriate personnel security control.

4. Assets received from or exchanged with external partners MUST be protected in accordance with any relevant legislative or regulatory requirements, including any international agreements and obligations.

Government Security Classifications

OFFICIAL

Majority of information processed by public sector

- This includes routine business operations and services, some of which could have damaging consequences if lost, stolen or published in the media, but are not subject to a heightened threat profile.

Government Security Classifications

OFFICIAL - SENSITIVE

OFFICIAL information that could have more damaging consequences

- A limited subset of OFFICIAL information could have more damaging consequences (for individuals, an organisation or government generally) if it were lost, stolen or published in the media. This subset of information should still be managed within the 'OFFICIAL' classification tier, but may attract additional measures (generally procedural or personnel) to reinforce the 'need to know'. In such cases where there is a clear and justifiable requirement to reinforce the 'need to know', assets should be conspicuously marked: 'OFFICIAL–SENSITIVE' .

Government Security Classifications

SECRET

Very sensitive information

- Justifies heightened protective measures to defend against determined and highly capable threat actors. For example, where compromise could seriously damage military capabilities, international relations or the investigation of serious organised crime.

Government Security Classifications

TOP SECRET

HMG's most sensitive information

- Requiring the highest levels of protection from the most serious threats. For example, where compromise could cause widespread loss of life or else threaten the security or economic wellbeing of the country or friendly nations.

Breaches

What is a breach?

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Personal data breaches can include:

- Data theft, loss or access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- Hacking or denial of service to computing systems containing personal data
- alteration of personal data without permission; and
- loss of availability of personal data.

All organizations have a duty to report certain types of personal data breach to the ICO within 72 hours of becoming aware of the breach, where feasible.

Breaches

OPCC Responsibility

- OPCC is expected to implement institutional mechanisms that can ensure the protection of personal data and this includes the prevention and management of data breaches should they occur.

All organizations have a duty to report certain types of personal data breach to the ICO within 72 hours of becoming aware of the breach, where feasible.

Breaches

Your Responsibility

- Should a breach occur, it is very important for you to notify the OPCC data protection team immediately. This notification is by sending an email to the OPCC Data Protection Officer, on dpo@westyorkshire.pcc.pnn.gov.uk

All organizations have a duty to report certain types of personal data breach to the ICO within 72 hours of becoming aware of the breach, where feasible.

Breaches

Your Responsibility

When reporting, you must include the following information:

- Date of incident discovery.
- Date of actual incident and the location.
- Name of person reporting the incident.
- Contact details of person reporting the incident (Email & phone number).
- Short description of the breach incident and data affected.
- Total number of data subjects involved in breach (if known).
- State if any personal data has been breached (provide details).
- Comment on actions taken at the time of data breach.

All organizations have a duty to report certain types of personal data breach to the ICO within 72 hours of becoming aware of the breach, where feasible.

Part 2

WY – OPCC
Data Protection Training
Jan, 2019

Records Retention

Personal data must not be kept longer than is necessary for the purposes for which it is processed.

- Must be able to justify how long data is kept for depending on the purpose
- Periodically review the data held , and erase or anonymise it when it is no longer needed
- Must carefully consider any challenges to retention of data. Individuals have a right to erasure if the data is no longer needed.
- Can be kept tor longer if keeping it for public interest archiving, scientific or historical research, or statistical purposes