Bath & North East Somerset Council

Have you been Hacked?

- In 2014 60% of small businesses experienced a cyber breach
- The average cost of the worse breaches was £65,000 to £115,000
  - Financial losses from theft of information, financial and bank details or money.
  - Financial losses from disruption to trading and doing business, especially if you are dependent on doing business online. The worst breaches can result in a business being put of action for up to 10 days.
  - Losing business from bad publicity & damage to your reputation & customer base.
  - Costs from cleaning up affected systems and getting them up and running.
  - Costs of fines if personal data is lost or compromised.
  - Damage to other companies that you supply or are connected to.

Bath & North East Somerset Council

Three simple things to improve online security

- Make your passwords stronger
- Install security software on all devices
- Always download the latest software updates

Bath & North East Somerset Council

Cyber/IT Security

Organisations need to have:

- IT Security Policy
- Security products for malware, anti-virus, etc
- An acceptable use policy for staff
- Appropriately security checked and trained staff
- Access and leaver controls
- Annual penetration test of system

10 Steps To Cyber Security

CESG

Defining and communicating your Board's Information Risk Management Regime is central to your organisation's overall cyber security strategy. CESG recommend you review this regime - together with the nine associated security areas described below - in order to protect your business against the majority of cyber threats.

User Education and Awareness

Produce user security policies covering acceptable and secure use of the organisation's systems. Establish a staff training programme. Maintain user awareness of the cyber risks.

Network Security

Protect your networks against external and internal attack. Manage the network perimeter. Filter out unauthorised access and malicious content. Monitor and test security controls.

Home and Mobile Working

Develop a mobile working policy and train staff to adhere to it. Apply the secure baseline build to all devices. Protect data both in transit and at rest.

Establish an effective governance structure and determine your risk appetite.

Information Risk Management Regime

Malware Protection

Produce relevant policy and establish anti-malware defences that are applicable and relevant to all business areas. Scan for malware across the organisation.

Secure Configuration

Apply security patches and ensure that the secure configuration of all ICT systems is maintained. Create a system inventory and define a baseline build for all ICT devices.

Maintain the Board's engagement with the cyber risk.

Produce supporting information risk management policies.

Removable Media Controls

Produce a policy to control all access to removable media. Limit media types and use. Scan all media for malware before importing on to the corporate system.

Monitoring

Establish a monitoring strategy and produce supporting policies. Continuously monitor all ICT systems and networks. Analyse logs for unusual activity that could indicate an attack.

Managing User Privileges

Establish account management processes and limit the number of privileged accounts. Limit user privileges and monitor user activity. Control access to activity and audit logs.

Incident Management

Establish an incident response and disaster recover capability. Produce and test incident management plans. Provide specialist training to the incident management team. Report criminal incidents to law enforcement.

Department for Business Innovation & Skills

CPNI Centre for the Protection of National Infrastructure

Cabinet Office

Bath & North East Somerset Council

Standards

- Cyber Essential Scheme
- ISO27001
- For small businesses – https://cyberstreetwise.com/
- Compliance with relevant technical standards
- Cyber incident response process
- Baseline personnel security standard (if processing personal or sensitive information)
- CESG 10 steps to cyber security (https://www.cesg.gov.uk/10-steps-cyber-security)
- Hosted systems questionnaire

Bath & North East Somerset Council

Useful Links

- 10 steps to Cyber Security
  - https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility/10-steps-summary
- Cyber Essentials
  - http://www.cyberessentials.org/
- CyberStreetWise
  - https://www.cyberstreetwise.com/

Bath & North East Somerset Council

So why is this important?

Bath & North East Somerset Council

Information Governance (IG)

A framework for managing information

- confidentially
- securely

taking into account

- ethical
- legal
- quality standards

Governed by the Data Protection Act 1998 which ensures:

- personal information is handled properly
- legal rights to people who have information stored about them

Bath & North East Somerset Council

Personal & Sensitive Data

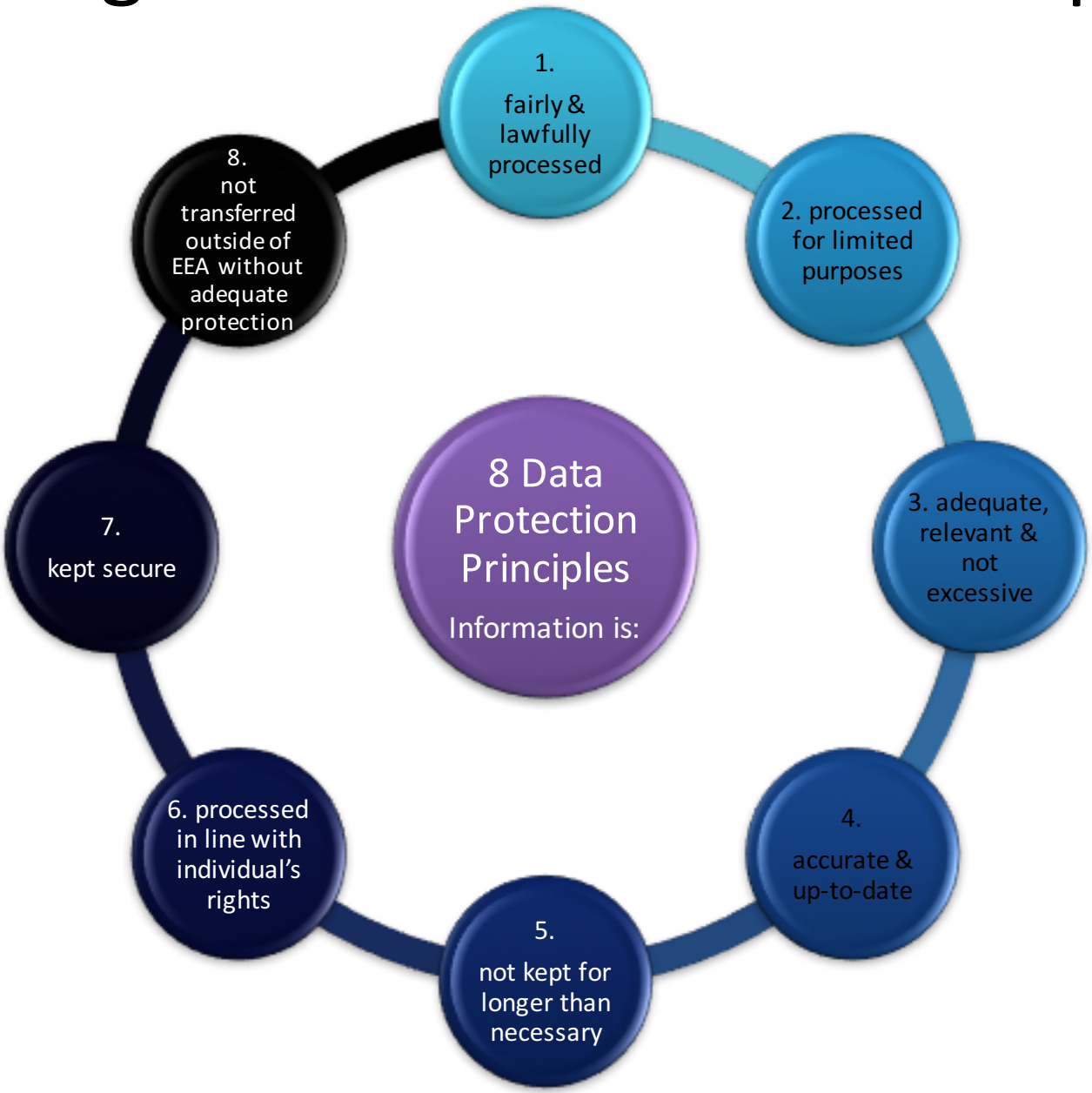
Personal data relating to a living individual who can be identified:

- from those data
- or other information in the possession (or likely to be) of the data controller
- and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual

Sensitive personal data, eg (not exhaustive list):

- racial/ethnic origin
- member of a trade union
- physical/mental health
- any offences committed
- etc

The Eight Data Protection Principles



Bath & North East Somerset Council

Why is this taken seriously?

- Reputation
  - Any breaches of the DPA by us or our partners (suppliers) can lead to poor reputation
- Trust
  - A lack of trust by service users can lead to a lack of information and thus poor decision making & service users not obtaining the support needed
- Information Commissioner's Office
  - The UK regulatory body who has an array of powers in relation to breaches of the DPA

Bath & North East Somerset Council

Relevance to Procurement

- DP/IG applies to any procurement & contract where personal and/or sensitive personal data will be processed in some way. For example:
  - Service providers
  - IT systems
- Where relevant IG questions will be asked at PQQ/ITT stages
- Will be subject to ongoing contract management review

Bath & North East Somerset Council

Thank you!

Richard Howroyd

richard_howroyd@bathnes.gov.uk