Better value, delivered.

Data Protection Policy

www.ypo.co.uk

Document Control Page

Document Type	Policy	
Document Ownership	Executive Director	
Title of Document	Data Protection Policy	
Status	Final	
Reference number	DP16062015	
Controlled by	Executive Director	
Created/ reviewed by / date:	Risk Audit and Assurance Officer	June 2015
Agreed by / date:	Board of Directors	16th June 2015
Checked for compliance with contract standing orders and financial procedures / date:		June 2015
Maintained by	Risk Audit and Assurance Officer	
Publication date	June 2015	
Next Review date	June 2015	
Current Version	DP16062015	
Distribution	All, intranet, website	
Replaces document	DPP20140224	

Once printed, this document is uncontrolled. Please refer to the current version on the Intranet.

Data Protection Policy

Contents

1. Introduction

1.1. The Data Protection Act 1998 (DPA) establishes a framework of rights and duties which are designed to safeguard personal data. This framework balances the legitimate needs of the organisation to collect and use personal data for business and other purposes against the right of individuals to respect for the privacy of their personal details. The legislation is underpinned by a set of eight straightforward common-sense principles.

1.2. The Act applies to a particular activity – processing personal data – rather than to particular people or organisations, so if you "process personal data" then you must comply with the Act and, in particular, you must handle the personal data in accordance with the data protection principles. Broadly, if you collect or hold information about an identifiable living individual, or if you use, disclose, retain or destroy that information, you are likely to be processing personal data. The scope of the Data Protection Act is therefore very wide as it applies to just about everything you might do with an individual's personal details.

1.3. The eight data protection principles are as follows:

1. Principle 1 - Processing Personal Data Fairly and Lawfully

"Personal data shall be processed fairly and lawfully"

In practice this means that you must:

- have legitimate grounds for collecting and using personal data
- not use the data in ways that have unjustified adverse effects on the individuals concerned
- be transparent about how you intend to use the data, and give individuals appropriate privacy notices when collecting their personal data
- handle people's personal data only in ways they would reasonably expect; and
- make sure you do not do anything unlawful with the data.

2. Principle 2 - Processing Personal Data For Specified Purposes

"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"

In practice the second data protection principle means that you must:

- be clear from the outset about why you are collecting personal data and what you intend to do with it
- comply with the Act's fair processing requirements – including the duty to give privacy notices to individuals when collecting their personal data
- comply with what the Act says about notifying the Information Commissioner; and
- ensure that if you wish to use or disclose the personal data for any other purpose that is additional to or different from the originally specified purpose, the new use or disclosure is fair.

3. **Principle 3 - Information Standards: The Amount of Personal Data You May Hold**

   The Act Says "*Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed*".

   In practice it means you should ensure that:
   - you hold personal data about an individual that is sufficient for the purpose you are holding it for in relation to that individual; and
   - you do not hold more information than you need for that purpose.

4. **Principle 4 - Information Standards: Keeping Personal Data Accurate and Up To Date**

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

   To comply with these provisions you should:
   - take reasonable steps to ensure the accuracy of any personal data you obtain
   - ensure that the source of any personal data is clear
   - carefully consider any challenges to the accuracy of information; and
   - consider whether it is necessary to update the information.

5. **Principle 5 - Information Standards: Retaining Personal Data**

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

   In practice, it means that you will need to:
   - review the length of time you keep personal data
   - consider the purpose or purposes you hold the information for in deciding whether (and for how long) to retain it
   - securely delete information that is no longer needed for this purpose or these purposes; and
   - update, archive or securely delete information if it goes out of date.

6. **Principle 6 - The Rights of Individuals**

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

   The Data Protection Act gives rights to individuals in respect of the personal data that organisations hold about them. This is the sixth data protection principle, and the rights of individuals that it refers to are:
   - a right of access to a copy of the information comprised in their personal data
   - a right to object to processing that is likely to cause or is causing damage or distress
   - a right to prevent processing for direct marketing
   - a right to object to decisions being taken by automatic means
   - a right in certain circumstances to have inaccurate personal data rectified, blocked, erased or destroyed; and
   - a right to claim compensation for damages caused by a breach of the Act.

7. **Principle 7 - Information Security**

   The Data Protection Act says that:

   "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"

   In practice, it means you must have appropriate security to prevent the personal data you hold being accidently or deliberately compromised. In particular, you will need to:
   - design and organise your security to fit the nature of the personal data you hold and the harm that may result from a security breach
   - be clear about who in your organisation is responsible for ensuring information security
   - make sure you have the right physical and technical security, backed up by robust policies and procedures and reliable, well trained staff; and
   - be ready to respond to any breach of security swiftly and effectively.

8. **Principle 8 - Sending Personal Data Outside The European Economic Area**

   "Personal data shall not be transferred to a country or territory outside the EU unless the country ensures an adequate level of protection for the rights and freedom of data subjects in relation to the processing of personal data"

   This is the eighth data protection principle, but other principles of the Act will also usually be relevant to sending personal data overseas.

1.4. The following are definitions of terms used in the Act.

Data means information which is being processed by means of equipment operating automatically in response to instructions given for that purpose or is recorded with the intention that it should be processed by means of such equipment, is recorded as part of a filing system or with the intention that it should form part of such a filing system, Information which forms part of an accessible record or recorded information held by a public authority which does not fall into any of the categories above.

Personal Data means data which relates to a living individual who can be identified from the data.

Sensitive Personal Data means personal data consisting of information as to racial or ethnic origin of the data subject, his political opinions, his religious beliefs or other beliefs of a similar nature, whether he is a member of a trade union, his physical or mental health or condition, his sexual life, the commission or alleged commission by him of any offence, or any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

Data Subject means an individual who is the subject of personal data.

Data Controller means an individual or organisation who determines the purposes for which and the manner in which any personal data is to be processed. YPO is a Data Controller.

Data Processor means any person (other than an employee of the data controller) who processes data on behalf of the data controller.

Processing in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data.

1.5. The Information Commissioners Office (ICO) is the UK's independent authority who upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The Information Commissioner has responsibilities in respect of Freedom of Information as well as Data Protection.

1.6. The Data Protection Act makes the Information Commissioner responsible for:
- promoting good practice in handling personal data and giving advice and guidance on data protection
- keeping a register of organisations that are required to notify him about their information-processing activities
- helping to resolve disputes by deciding whether it is likely or unlikely that an organisation has complied with the Act when processing personal data
- taking action to enforce compliance with the Act where appropriate; and
- bringing prosecutions for offences committed under the Act.

1.7. If you are processing personal data you usually have to notify the Information Commissioner about this. Failure to notify is a criminal offence. YPO is registered as a Data Controller.

1.8. Data sharing is the process of disclosing data from one or more organisations to a third party organisation or organisations, or the sharing of data between different parts of an organisation. Data sharing can take the form of:
- a reciprocal exchange of data;
- one or more organisations providing data to a third party or parties
- several organisations pooling information and making it available to each other
- several organisations pooling information and making it available to a third party or parties
- exceptional, one-off disclosures of data in unexpected or emergency situations; or
- different parts of the same organisation making data available to each other.

1.9. Some data sharing doesn't involve personal data, for example where only statistics that cannot identify anyone are being shared. The Data Protection Act does not apply to this type of data sharing.

1.10. The Information Commissioner has produced a Data Sharing Code of Practice. The code covers the two main types of data sharing:
- systematic, routine data sharing where the same data sets are shared between the same organisations for an established purpose; and
- exceptional, one-off decisions to share data for any of a range of purposes.

1.11. The code explains how the DPA applies to the sharing of personal data. It also provides good practice advice that is relevant to all organisations that share personal data. Any data controller who is involved in the sharing of personal data should use this code to help them to understand how to adopt good practice.

2. Data Protection Do’s and Don’ts

- Do treat personal data with care.

- Do check identities before disclosing personal data. Where request are made for information about another individual ensure you have the consent of that individual prior to releasing the information.
- Do secure all personal data and dispose of confidential waste by placing it in the shredding consoles in the offices or the shredding bins in the warehouse.
- Do ensure your pc is password protected and always locked when you leave your desk.
- Do ensure that no one else, especially members of the public, can read information from your computer screen.
- Do ensure that personal data is not left on your desk – lock it away before you leave.
- Don't use unauthorised software on your PC.
- Don't tell anyone your password.
- Do not leave confidential papers on shared printers.
- Do ensure all personal information on laptops is secure and that laptops are stored securely at all times. Laptops should not be left in vehicles.
- Do ensure information passing between the offices or third parties is handled securely to ensure it does not go astray or is misdirected.
- Do not be tricked into giving away information, either about customers or colleagues, especially over the phone, through "social engineering".
- Do ensure all mobile technology (phones, laptops, tablets for example) are password protected.
- Do inform IT immediately of any loss of equipment.
- Do ensure all personal information is adequately protected prior to sending (ie) password protection, encryption of files, USB's, disks etc.
- Do ensure any third parties handling data on our behalf have adequate data protection measures in place.
- Do ensure any data sharing is done in line with the ICO's Data Sharing Code of Practice.
- Do not transfer any personal data outside the EU without ensuring adequate controls are in place.
- Do only use personal data for the purpose it was collected for and always ensure you have consent to use it in this way.
- Do only disclose to those people with a need and a right to know.
- **If in doubt do not disclose personal data and check with the Data Protection Officer.**

3. Purpose of the Policy

3.1. The purpose of this policy is to enable YPO to:
   - comply with the law in respect of the data it holds about individuals
   - follow good practice
   - protect YPO's stakeholders, staff and other individuals; and
   - protect the organisation from the consequences of a breach of its responsibilities.

4. Data Protection Act 1998 Policy Statement

DATA PROTECTION ACT 1998 POLICY STATEMENT

.

YPO is the UK's largest public sector buying organisation, with a customer base including schools and wider education establishments, emergency services and local authorities.

YPO needs to collect and use certain types of information about people with whom it deals in order to operate. These include current, past and prospective customers, YPO's own employees, suppliers and others with whom YPO conducts business. In addition, YPO may occasionally be required by law to collect and use certain types of information to comply with the requirements of government departments. This information may be held electronically or in paper files. This personal information must be dealt with properly however it is collected, recorded and used – whether on paper, electronically, or other means - and there are safeguards to ensure this in the Data Protection Act 1998.

We regard the lawful and correct treatment of personal information by YPO as important to the achievement of our objectives and to the success of our operations, and to maintaining confidence between those with whom we deal and ourselves. We therefore need to ensure that our organisation treats personal information lawfully and correctly. To this end, we fully endorse and adhere to the principles of data protection, as set out in the Data Protection Act 1998.

The Data Protection Act 1998 requires that personal data is:

1. processed fairly and lawfully
2. 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. shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed
4. accurate and, where necessary, kept up to date
5. not kept for longer than is necessary for that purpose or those purposes
6. 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. not transferred to a country or territory outside the EU unless the country ensures an adequate level of protection for the rights and freedom of data subjects in relation to the processing of personal data.

Therefore, YPO will, through appropriate management and strict application of criteria and controls:

- Observe fully conditions regarding the fair collection and use of information.
- Meet its legal obligations to specify the purposes for which information is used.
- Collect and process appropriate information only to the extent that it is needed to fulfil our operational needs or to comply with any legal requirements.
- Ensure the quality of information used.
- Ensure that the information is held for no longer than is necessary.
- Ensure that the rights of people about whom information is held can be fully exercised under the Act (i.e. the right to be informed that processing is being undertaken, to access one's personal information; to prevent processing in certain

circumstances, and to correct, rectify, block or erase information that is regarded as wrong information).
- Take appropriate technical and organisational security measures to safeguard personal information; and
- Ensure that personal information is not transferred abroad without suitable safeguards.

The Board of Directors recognises its overall responsibility for ensuring that YPO complies with its legal obligations.

Signed: Simon Hill, MD Date: 16th June 2015

5. Roles and Responsibilities

5.1. Everyone has a role to play in ensuring personal data remains secure and YPO expects all of its employees to lead by example. The expectation is that employees of all levels will adopt the highest standards in relation to data protection and demonstrate that YPO is acting in a transparent and honest manner. YPO also expects organisations and individuals that deal with YPO to operate to the same

high standards in relation to data protection and abide by YPO's policies, procedures and guidance as appropriate.

5.2. The Board of Directors recognises its overall responsibility for ensuring that YPO complies with its legal obligations and will ensure adequate resources are made available for the effective implementation of this policy and associated processes.

5.3. The nominated Officer for Data Protection holds the following responsibilities:
- Briefing the board on data protection responsibilities.
- Reviewing data protection and related policies.
- Advising staff on data protection issues.
- Ensuring that data protection training takes place.
- Notification.
- Handling subject access requests.
- Approving unusual or controversial disclosures of personal data.
- Approving contracts with Data Processors.

5.4. The day to day responsibility for data protection rests with Line Managers and Heads of Department who are responsible for:
- Identifying the risks to which personal data is exposed to.
- Developing and maintaining effective controls to ensure information security, accuracy of data, fair processing and any other requirements under the data protection act; and
- Ensuring fair processing notices are in place outlining what and how information is going to be processed. This is to make sure the individual knows exactly what is going to happen to their information and how it is going to be used. A fair processing notice (or privacy notice) is an oral or written statement that individuals are given when information about them is collected You shouldn't be doing anything with personal information unless the individual is made aware (unless certain exemptions apply).
- Ensuring access to personal data and confidential files on the IT network is restricted.
- Ensuring that controls are being complied with.

5.5. Each department where personal data is handled is responsible for drawing up its own operational procedures to ensure that good data protection practice is established and followed within their departments. Relevant Managers of the departments must ensure that the nominated Officer for Data Protection is informed of any changes in their uses of personal data that might affect the organisation's Notification.

5.6. If significant risks / breaches are identified then these shall be immediately notified to Senior Management and thenominated Officer for Data Protection. These should also be included in Divisional Risk Registers with a view to ensuring they are regularly monitored.

5.7. Managers should ensure that all employees are aware of YPO's Data Protection Policy and Procedures.

5.8. All staff, including Managers and Heads of Departments are responsible for adhering to the various policies, procedures and work instructions to their role in relation to data protection and ensuring that they always comply fully with the provisions of the Data Protection Act.

5.9. YPO will identify any personal data processed by the organisation and the uses of this personal data to ensure systems and controls remain adequate. It is the responsibility of Managers (including Heads of Department) to ensure that data use identification is completed for their department by the completion of a Data Protection Data Use Questionnaire (see annex 1).

5.10. Employees for YPO may need to have access to personal information which may include, for example:

- Personal information about individuals who are customers or otherwise involved in the activities organised by YPO.
- Information about the internal business of YPO.
- Personal information about colleagues working for YPO.

YPO is committed to keeping this information confidential, in order to protect individuals and YPO itself. 'Confidential' means that all access to information must be on a need to know and properly authorised basis. You must use only the information you have been authorised to use, and for purposes that have been authorised. You should also be aware that under the Data Protection Act, unauthorised access to data about individuals is a criminal offence.

5.11. All staff must assume that information is confidential unless you know that it is intended by YPO to be made public.

5.12. All staff must also be particularly careful not to disclose confidential information to unauthorised people or cause a breach of security. In particular staff must:

- Not compromise or seek to evade security measures (including computer passwords).
- Be particularly careful when sending information between offices and third parties.
- Not gossip about confidential information, either with colleagues or people outside YPO.
- Not disclose information — especially over the telephone — unless you are sure that you know who you are disclosing it to, and that they are authorised to have it.
- Be careful when sending information to shared printers and ensure this information is promptly collected.
- Not transfer information in relation to individuals onto personal pc's or storage devices.
- Put any information to be disposed of into the shredding consoles in the offices or shredding bins in the warehouse

5.13. All employees are responsible for ensuring that any disclosure of data from YPO to a third party organisation or organisations, or the sharing of data between different parts of YPO complies with the Information Commissioners Data Sharing Code of Practice.

5.14. If employees are in doubt about whether to disclose information or not, do not guess. Withhold the information while you check with the nominated Officer for Data Protection whether the disclosure is appropriate.

5.15. All employees must ensure documents containing personal data or of a sensitive or confidential nature are securely disposed of by putting them in the shredding consoles in the offices or shredding bins in the warehouse.

5.16. All employees are required to read, understand and accept any policies and procedures that relate to the personal data they may handle in the course of their work.

5.17. All employees are responsible for ensuring that any direct marketing is carried out in accordance with The Data Protection Act and any associated rules. Because data subjects have the right to require their data not to be used for marketing, it is good practice to make it clear when there is an intention to use their data for marketing and offer them an opt-out (via a tick-box or an easy-to-use alternative) at the earliest opportunity.

5.18. Significant breaches of this policy may be handled under YPO's disciplinary procedures.

5.19. YPO will regularly review its procedures for ensuring that its records remain accurate and consistent and, in particular:

- ICT systems will be designed, where possible, to encourage and facilitate the entry of accurate data.
- Data on any individual will be held in as few places as necessary, and all staff will be discouraged from establishing unnecessary additional data sets.
- Effective procedures will be in place so that all relevant systems are updated when information about any individual changes.

5.20. YPO will ensure that all mobile technology (phones, laptops, tablets for example) have adequate encryption and password protection. Employeesshould not attempt to override these systems.

5.21. All employees shall consider the data protection risks involved in any projects prior to embarkation and ensure arrangements are formalised to ensure compliance with the Act.

5.22. All ICT systems will be designed and sourced ensuring compliance with the eighth principle of data protection in relation to sending personal data outside the European Union.

5.23. Some categories of data must be held for a period of time to meet legal requirements. The Information and Records Management Society maintains retention guidelines online however these should be used as a guide only and further advice taken if there is any doubt about the retention period.

6. Subject Access Requests

6.1. The right, commonly referred to as subject access,is most often used by individuals who want to see a copy of the information an organisation holds about them. However, the right of access goes further than this and an individual who makes a written request and pays a fee is entitled to be:

- Told whether any personal data is being processed.
- Given a description of the personal data, the reasons it is being processed, and whether it will be given to any other organisations or people.
- Given a copy of the information comprising the data; and
- Given details of the source of the data (where this is available).

6.2. An individual can also request information about the reasoning behind any automated decisions, such as computer-generated decision to grant or deny

credit, or an assessment of performance at work (except where this information is a trade secret).

6.3. In most cases you must respond to a subject access request promptly and in any event within 40 calendar days of receiving it. However, some types of personal data are exempt from the right of subject access and so cannot be obtained by making a subject access request.

6.4. Under the right of subject access, an individual is entitled only to **their own** personal data, and not to information relating to other people (unless they are acting on behalf of that person and have that persons consent). Neither are they entitled to information simply because they may be interested in it, so it is important to establish whether the information requested falls within the definition of personal data. In most cases, it will be obvious whether the information being requested is personal data, but the ICO have produced separate guidance to help you decide in cases where it is unclear. Subject access provides a right to see the information contained in personal data, rather than a right to see the documents that include that information. Various exceptions to the right of subject access apply in certain circumstances or to certain types of personal data.

6.5. For a subject access request to be valid, it should be made in writing. You should also note the following points when considering validity:

- A request sent by email or fax is as valid as one sent in hard copy.
- You do not need to respond to a request made verbally but, depending on the circumstances, it might be reasonable to do so (as long as you are satisfied about the person's identity), and it is good practice to at least explain to the individual how to make a valid request, rather than ignoring them.
- If a request does not mention the Act specifically or even say that it is a subject access request, it is nevertheless valid and should be treated as such if it is clear that the individual is asking for their own personal data.
- A request is valid even if the individual has not sent it directly to the person who normally deals with such requests – so it is important to ensure that you and your colleagues can recognise a subject access request and treat it appropriately. All Subject access requests received within YPO should be forwarded immediately to the nominated Officer for Data Protection. .

6.6. YPO may charge £10.00 for dealing with subject access requests. The individual is also required to prove their identity prior to any information being released. If a request is made by a third party we must have the written consent of the individual concerned prior to releasing any information.

6.7. To ensure all subject access requests are handled correctly all requests should be passed immediately to the nominated Officer for Data Protection . All staff are required to pass on anything which might be a subject access request to the nominated Officer for Data Protection without delay.

6.8. The Freedom of Information Act (FOI) deals with information held by public authorities. The Act gives individuals the right to request information held by public authorities, unless there are good reasons to keep it confidential. As well as subject access requests YPO may also receive FOI requests. To ensure all FOI requests are handled correctly all staff are required to pass on anything which

might be an FOI request immediately to the nominated Officer for Freedom of Information. Please refer to YPO's Access to Information Policy for further information.

7. Contact With Law Enforcement Agencies

7.1. There may be occasions when YPO is contacted by law enforcement agencies requesting information. To protect YPO and to ensure these requests are handled appropriately all such requests must be passed immediately to nominated Officer for Data Protection to ensure we have the necessary safeguards in place prior to any information being released.

7.2. To prevent prejudicing any criminal investigation and the possibility of prosecution for tipping off you must also ensure that you tell no other party about the request, including the person about whom the information was requested. Tipping off is an offence under the Proceeds of Crime Act and may be punishable by a fine and/or a prison sentence.

8. Maintaining and Reviewing Data Protection Arrangements

8.1. YPO's data protection policies and procedures will be regularly reviewed to ensure they are up to date and effective in allowing YPO to comply with the provisions of the Data Protection Act.

8.2. Individual department's data protection procedures will be maintained by the Head of Department to ensure they reflect current process / activity. Amendments to procedures may be required due to changes in processes, activities, staff, department structures, the external environment and legislative changes.

8.3. To ensure compliance with the Data Protection Act becomes a part of YPO's core values YPO will raise, enhance and maintain awareness through an ongoing DPA

education and information programme for all employees and establish a process for evaluating the effectiveness of all DPA awareness delivery.

8.4. YPO will communicate to all employees the importance of meeting data protection objectives, conforming to the Data Protection Policy and continually improving in the area of data protection.

8.5. In the event of an incident that results in the invocation of the Data Breach Response Plan a post incident review shall be completed to assess the adequacy of the response and identify any required improvements to be made to the DPA arrangements.

9. Data Breach Response Plan

9.1. YPO has compiled a Data Breach Response Plan in order to define strategy that will be adopted in the event of a data breach.

9.2. A data breach may happen for a number of reasons:

- Loss or theft of data or equipment on which data is stored
- Inappropriate access controls allowing unauthorised use
- Equipment failure
- Human error
- Unforeseen circumstances such as a fire or flood
- Hacking attack

- ‘Blagging’ offences where information is obtained by deceiving the organisation who holds it.

9.3. This plan comprises of four elements:

1. Containment and recovery
2. Assessment of ongoing risk
3. Notification of breach
4. Evaluation and response

9.4. **Containment and Recovery**

9.4.1. The individual who identified the breach should determine whether the breach is ongoing (e.g., a hacker still accessing the data) and, if so, have IT shut it down.

9.4.2. All breaches should be **immediately** notified to The Incident Commander using the procedure laid down in the YPO Incident Management Plan. The Incident Commander with assistance from the nominated Officer for Data Protection will take the lead on investigating the breach.

9.4.3. The Incident Commanders will establish who from the Incident Managers or Incident Team Members needs to be made aware of the breach and inform them of what they are expected to do to assist in the containment exercise. This could be isolating or closing a compromised section of the network, finding a lost piece of equipment or simply changing the access codes on the doors.

9.4.4. The Incident Managers and Incident Team Members will establish whether there is anything YPO can do to recover any losses and limit the damage the breach will cause. As well as the physical recovery of equipment, this may involve the use of back-up tapes to restore lost or damaged data or ensuring that staff recognise when someone tries to use stolen data to access information.

9.5. **Assessing the ongoing risks**

9.5.1. Some data security breaches will not lead to risks beyond possible inconvenience to those who need the data to do their job. An example might be where a laptop is irreparably damaged but its files were backed up and can be recovered, albeit at some cost to the business. While these types of incidents can still have significant consequences the risks are very different from those posed by, for example, the theft of a customer / employee database, the data on which may be used to commit identity fraud. Before deciding on what steps are necessary further to immediate containment, assess the risks which may be associated with the breach.

9.5.2. YPO should ascertain:

- What type of data is involved? Does it relate to individuals or organisations?
- How sensitive is it? Remember that some data is sensitive because of its very personal nature (health records) while other data types are sensitive because of what might happen if it is misused (bank account details).
- If data has been lost or stolen, are there any protections in place such as encryption?

- What has happened to the data? If data has been stolen, it could be used for purposes which are harmful to the individuals to whom the data relate; if it has been damaged, this poses a different type and level of risk.
- Regardless of what has happened to the data, what could the data tell a third party about the individual? Sensitive data could mean very little to an opportunistic laptop thief while the loss of apparently trivial snippets of information could help a determined fraudster build up a detailed picture of other people.
- How many individuals' personal data are affected by the breach? It is not necessarily the case that the bigger risks will accrue from the loss of large amounts of data but is certainly an important determining factor in the overall risk assessment.
- Who are the individuals whose data has been breached? Whether they are staff, customers, clients or suppliers, for example, will to some extent determine the level of risk posed by the breach and, therefore, YPO's actions in attempting to mitigate those risks.
- What harm can come to those individuals? Are there risks to physical safety or reputation, of financial loss or a combination of these and other aspects of their life?
- Are there wider consequences to consider such as a risk to public health or loss of public confidence in an important service we provide?
- If individuals' bank details have been lost, consider contacting the banks themselves for advice on anything they can do to help YPO prevent fraudulent use.

9.6. Notification of Breaches

9.6.1. Informing people and organisations that YPO has experienced a data security breach is an important element in the breach management strategy. However, informing people about a breach is not an end in itself. Notification should have a clear purpose, whether this is to enable individuals who may have been affected to take steps to protect themselves or to allow the appropriate regulatory bodies to perform their functions, provide advice and deal with complaints.

9.6.2. YPO should answer the following questions to assist in deciding whether to notify:

- Are there any legal or contractual requirements? At present, there is no law expressly requiring you to notify a breach but sector specific rules may lead YPO towards issuing a notification.
- Can notification help YPO meet its security obligations with regard to the seventh data protection principle?
- Can notification help the individual? Bearing in mind the potential effects of the breach, could individuals act on the information YPO provides to mitigate risks, for example by cancelling a credit card or changing a password?
- If a large number of people are affected, or there are very serious consequences, YPO should inform the Information Commissioners Office.
- YPO should consider the dangers of 'over notifying'. Not every incident will warrant notification and notifying a whole employee base of an issue affecting only a few employees may cause disproportionate enquiries and work.

- YPO needs to consider who to notify, what we are going to tell them and how we are going to communicate the message. This will depend to a large extent on the nature of the breach.
- YPO should notify the appropriate regulatory body. A sector specific regulator may require YPO to notify them of any type of breach but the ICO should only be notified when the breach involves personal data.
- There are a number of different ways to notify those affected so YPO should use the most appropriate one. YPO should always bear in mind the security of the medium as well as the urgency of the situation.
- The notification should at the very least include a description of how and when the breach occurred and what data was involved. Include details of what YPO has already done to respond to the risks posed by the breach.
- When notifying individuals YPO should give specific and clear advice on the steps they can take to protect themselves and also what YPO is willing to do to help them.
- YPO should provide a way in which they can contact us for further information or to ask YPO questions about what has occurred – this could be a helpline number or a web page, for example.
- When notifying the ICO YPO should also include details of the security measures in place such as encryption and, where appropriate, details of the security procedures YPO had in place at the time the breach occurred. We should also inform the ICO if the media are aware of the breach so that they can manage any increase in enquiries from the public.
- When informing the media, it is useful to inform them whether YPO have contacted the ICO and what action is being taken. Any media contact should be dealt with by the Incident Commanders.
- ICO will not normally tell the media or other their parties about a breach notified to them, but they may advise YPO to do so.
- The ICO has produced guidance for organisations on the information they expect to receive as part of a breach notification and on what organisations can expect from them on receipt of their notification. This guidance is available on their website: **http://www.ico.gov.uk/Home/what_we_cover/data_protection/guidance/good_practice_notes.aspx**. The ICO can be contacted at:
  Information Commissioner's Office
  Wycliffe House
  Water Lane
  Wilmslow
  Cheshire SK9 5AF
  Tel: 0303 123 1113

9.6.3. YPO may also need to consider notifying third parties such as the police, insurers, trade unions, professional bodies, bank or credit card companies who can assist in reducing the risk of financial loss to individuals.

9.7. Bulk Protection Registration Service

9.7.1. If a data breach of personal data is severe YPO may consider using aBulk Registration Service or another similar scheme.

9.7.2. These services may allow those who are at risk of identity theft to have a special warning 'flag' placed on their credit reference agency file or enable an individual to monitor their credit file for any suspicious activity

9.7.3. .

9.7.4. Any contact with any party by YPO regarding bulk protective registration or similar scheme should first be authorised by the Incident Commander.

9.8. Evaluation and Response

9.8.1. Following a data breach it is vital to ensure that current policies and procedures are reviewed to ensure they are effective.

9.8.2. YPO's response to the incident should also be evaluated to ensure response arrangements are adequate.

Appendix 1

Data Protection Data Use Questionnaire

General Details	
Area	
Reference	
Description	
Project Risk Reference	
Company	
Department	

Section	
Location	
Assessor Name	
Date Of Assessment	
Question Set	Data Protection Data Use Questionnaire

Data Protection Questions		
Does your department process personal data on individuals? Personal data means data which relates to a living individual who can be identified from that data, or could be identified if the data was combined with other data		
Comments		
What personal information is collected? (eg) name, address, telephone number etc		
Comments		
Why do you hold this personal data?		
Comments		
Who are the data subjects? This is the type of individual who is the subject of personal data (eg) employees, customers etc		
Comments		
Please provide details of any databases or filing systems containing personal data		
Comments		
Do you hold any sensitive personal information (eg) medical or health data, ethnic origin etc? If so for what purpose?		
Comments		
How is this data collected?		
Comments		
Who is this personal data collected from? (eg) do you collect this directly from the individual or is it provided by a third party, for example another department		
Comments		

Do you use any fair processing notices when collecting the data? A fair processing notice is a written or oral statement detailing how information collected will be used. Please send copies of any notices used to The Data Protection Officer		
Comments		
Once personal data has been collected do you disclose this data to anyone? (If the answer is yes, please provide examples and reasons - this includes other departments within YPO as well as third parties)		
Comments		
How does your department store personal information? (eg) on computer or manual files or both etc		
Comments		
Is the information stored securely (eg) in a locked cabinet etc, please detail		
Comments		
Who has access to this information?		
Comments		

Please pass completed questionnaires to nominated Officer for Data Protection

Better value, delivered.

www.ypo.co.uk