PERSONAL DATA BREACH INCIDENT MANAGEMENT PROCEDURE

1. Purpose and Scope

1.1 This procedure is intended to supplement the University of Worcester's ("the University") Data Protection Policy and has been developed to aid members of the University understand the University's obligations in the event of a data breach.

1.2 This procedure applies to all members of the University. All contractors and agents acting for or on behalf of the University should be made aware of these guidelines and the University's Data Protection Policy.

1.3 The University is responsible for ensuring appropriate and proportionate security for the personal data it holds. This includes protecting the data against unauthorised or unlawful processing and against accidental loss, destruction or damage of that data.

1.4 In these cases it is important that the University responds appropriately. The University has a responsibility to deal with the breach immediately and appropriately in order to minimise the impact and prevent recurrence. Data protection legislation also imposes a requirement that most personal data breaches are reported to the Information Commissioner's Office within 72 hours of the University becoming aware of the breach.

2. Personal Data Breaches

2.1 A personal data breach is defined in data protection legislation to mean:

"a breach of security leading to the accidental or unlawful destruction, loss, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed."

2.2 Data Protection legislation sets out three categories of personal data breaches:

i) Confidentiality breach - where there is an unauthorised or accidental disclosure of, or access to, personal data;

ii) Integrity breach - where there is an unauthorised or accidental alternation of personal data;

iii) Availability breach - where there is an unauthorised or accidental loss of access to, or destruction of personal data.

2.3 The University makes every effort to avoid personal data breaches, however, it is possible that mistakes will occur on occasions or things will happen that are beyond the University's

control. A personal data breach can occur for a number of reasons some examples of these include:

- Loss or theft of data or equipment on which data is stored (even if the device is encrypted consideration needs to be given to whether there is a back-up available);
- Inappropriate access controls allowing unauthorised use;
- Equipment failure;
- Unauthorised disclosure (e.g. email sent to incorrect recipient or document posted to the wrong address or personal information posted on the website without consent);
- Human error;
- Unforeseen circumstances such as a fire or flood;
- Hacking attack;
- Marketing email sent to all recipients in the 'to' or 'cc' field instead of using 'bc' field;
- 'Blagging' offences where information is obtained by deceiving the organisation who holds it.

2.4 The consequences of a personal data breach could be physical, material or moral damage to individuals such as loss of control over their personal data, identify theft or fraud, financial loss, damage to the reputation, or any other economic or social disadvantage to the data subject concerned. The consequences of a personal data breach to the University include reputational risk and financial risks particularly in relation to the potential fines that may be imposed by the Information Commissioner's Office (ICO) of up to €20m or 4% of global turnover, whichever is higher.

3. Reporting an Incident

3.1 It is the responsibility of any member of staff, student or other individual who discovers a personal data breach, or believes a personal data breach may have occurred, to report it immediately - see Appendix 1 Flowchart for assessing who to advise of a potential data breach. Contact details for the University's Data Protection Officer are as follows:

Email: infoassurance@worc.ac.uk
and
during working hours call the Head of Information Assurance on
01905 855014 or 01905 855031
The Head of Information Assurance (Helen Johnstone) is the University's Data Protection Officer

On initial contact, the reporter should provide details of:

- The exact nature of the breach
- An indication of the seriousness of the breach (the sensitivity of the data breached, the number of individuals whose data may be involved, who may have access to the data)

- If possible the actions needed to be taken immediately to mitigate the breach.

3.2 The Head of Information Assurance, who is the University's Data Protection Officer will ask for the provision of more detailed follow up information (see Appendix 2 for further details) within 24 hours of the discovery of the breach.

3.3 It will be the responsibility of the University's Data Protection Officer, or their nominee in their absence, to assess the breach and decide whether to report the incident to the Information Commissioner's Office (Appendix 3 - Flowchart showing notification requirements). A decision to report, or not, needs to be made within 72 hours of the Data Protection Officer becoming aware of the breach. If a decision is taken not to report the breach or the report is delayed, the reasons for this needs to be recorded. Further information is available on the ICO's website.

3.4 The Data Protection Officer will contact other parties as required such as the University Secretary, the police if there has been any illegal activity or the Press Office if there is likely to be press interest. Other University departments will be notified as appropriate. In particular if the breach involves IT security, the IT Department will also be consulted. There may also be legal/contractual requirements to notify. The Data Protection Officer will advise if the data subject(s) should be advised of the breach.

4. Data Subjects

4.1 After a personal data breach is identified, the Data Protection Officer will assess whether the breach will result in a high risk to the rights and freedoms of the individual(s). If it is considered that there is a high risk to the individual(s) rights and freedoms then they will be notified as soon as is practicable by the most appropriate means.

4.2 The Data Protection Officer will communicate with the area of the University responsible for the data that has been breached and discuss the best way of contacting the data subjects concerned and what information the data subjects should be given.

4.3 When individuals are notified, they should be given the following information:

- Description of the nature of the breach;
- Name and contact details of the Data Protection Officer;
- Description of likely consequences of the breach;
- Description of measures taken or to be taken to address the breach;
- Specific information about steps the individual can take to protect themselves.

5. Containment and recovery

5.1 Steps should be taken as soon as possible to recover any losses and limit the damage. Steps might include:

- Attempt to recover lost equipment
- Attempt to retrieve personal data e.g. recall emails, remove from websites, etc.
- Use backups to recover lost, damaged or stolen data

- Change relevant passwords as soon as possible
- If bank details have been lost/stolen, contacting banks directly for advice on preventing fraudulent use

6. Evaluation and response

6.1 Once the incident is contained, a review should be conducted into the causes of the breach and the effectiveness of the response. The review should consider the type of data, what protections were in place (e.g. encryption), what happened to the data and whether there could be wider consequences of the breach. If ongoing problems are identified, then an action plan should be drawn up to put these right. In the case of the most serious breaches, a report will be submitted to the Audit Committee.

6.2 If a breach warrants a staff disciplinary investigation, HR will be contacted for advice and guidance.

6.3 The Data Protection Officer will keep a record of all data breaches including the actions taken to mitigate the breach and lessons learned. Details of information to be recorded relating to personal data breaches is available at Appendix 4

6.4 In the event that the University is responsible for causing a personal data breach, or not taking appropriate action to prevent a breach, then there could be financial consequences. It is therefore important to make every effort to prevent breaches occurring, and if breaches do occur, take required actions. More information about the impact of non-compliance can be found in para 1.2 of the Data Protection Policy

7. Other related documents and information

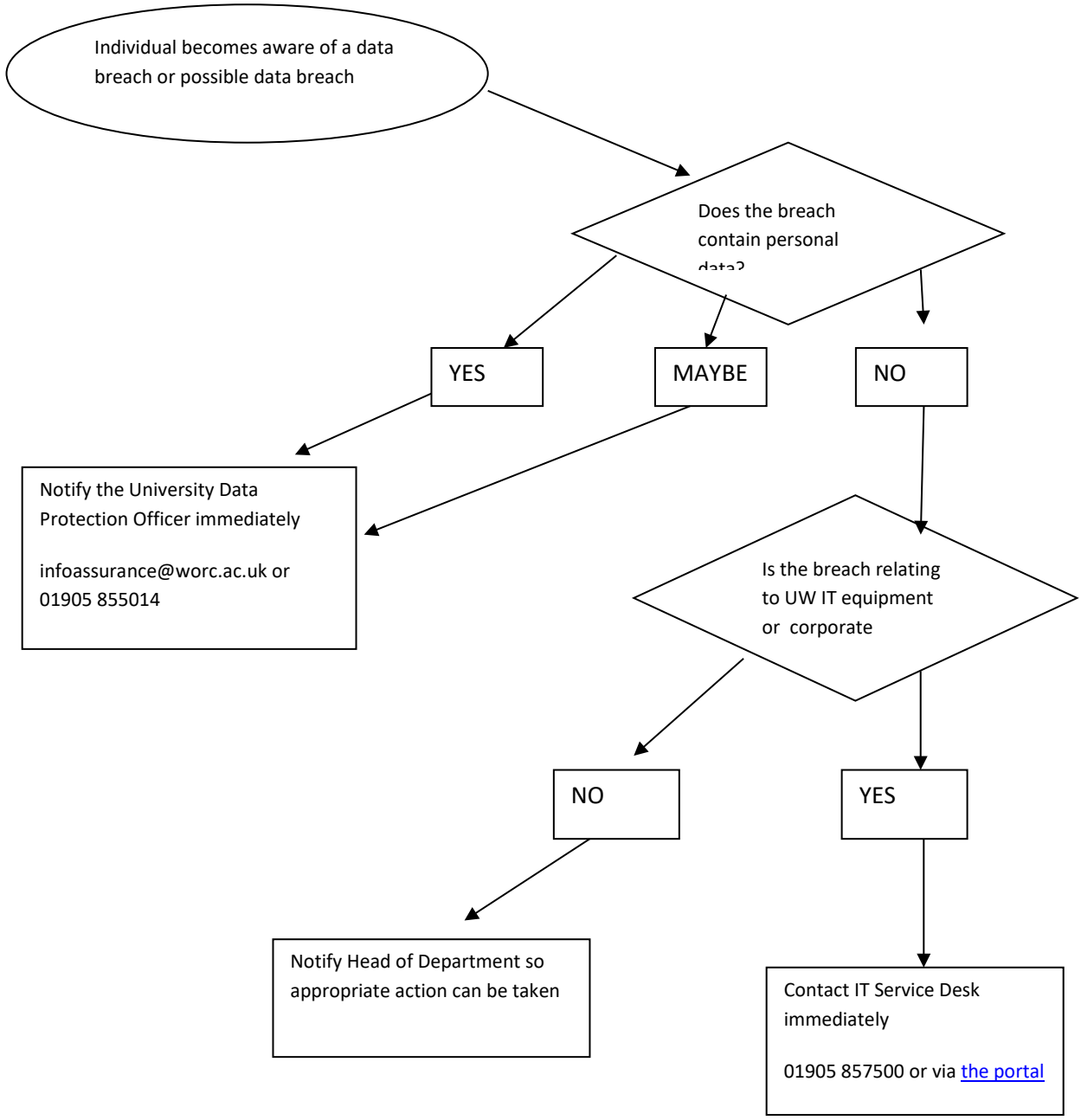
Data Protection Policy
Information Security Policy
IT Regulations
ICO advice on Data Breaches

Article 29 Working Party Guidance on Personal Data Breach Notification (Article 29 Working Group is an independent EU advisory body on data protection and privacy)

Version number	Version 1.0
Author/Originator	Head of Information Assurance
Review Date	1st May 2019
Ratified/Authorised by	VCAG
Issue date	25th May 2018
Postholder/s responsible for review	Head of Information Assurance

Appendix 1

What to do if you think there has been a data breach



Appendix 2

Internal Reporting requirements

The Data Protection Officer should be notified immediately in the event of a possible personal data breach.

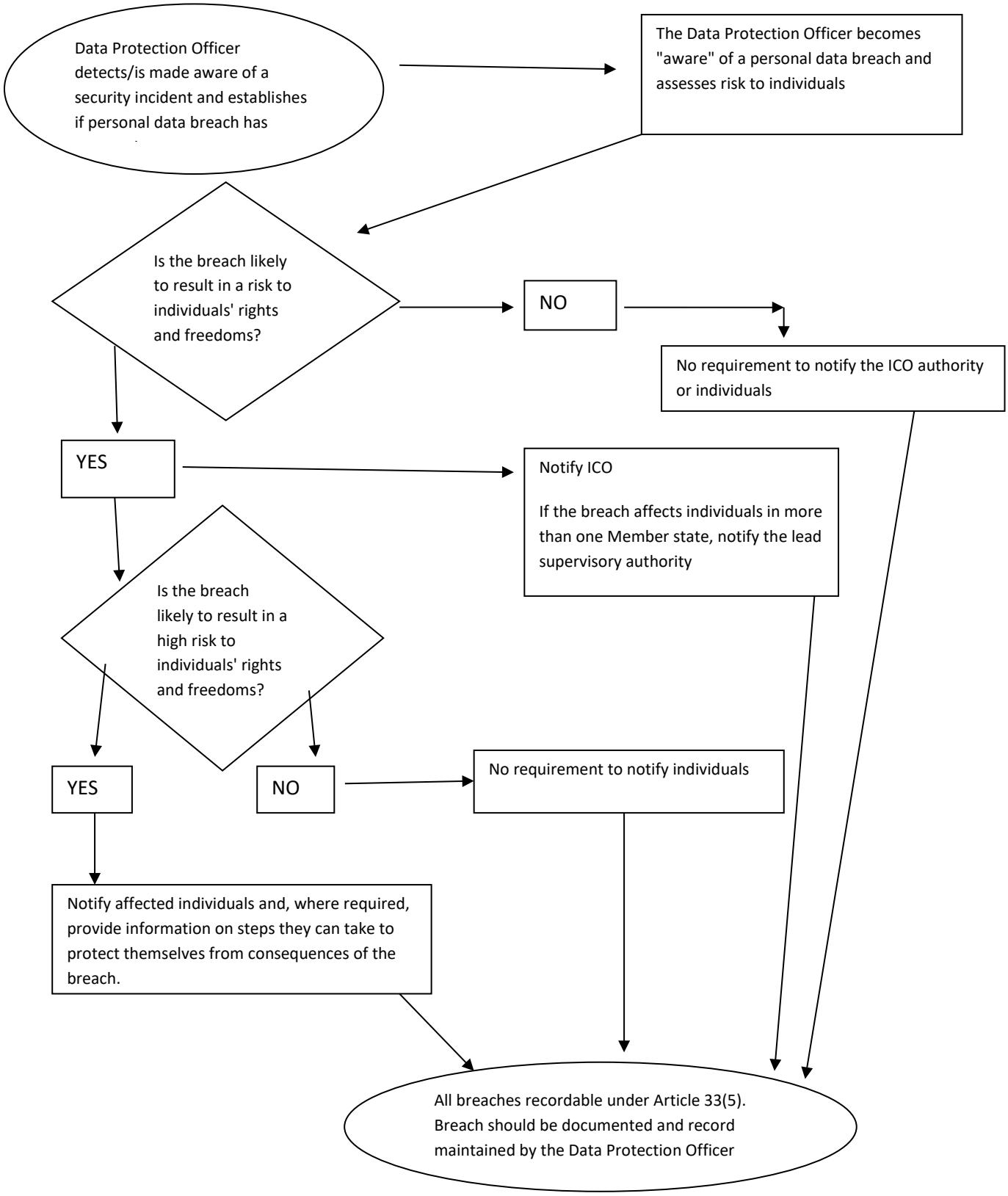
Email: infoassurance@worc.ac.uk
and
during working hours call the Head of Information Assurance on
01905 855014 or 01905 855031
The Head of Information Assurance (Helen Johnstone) is the University's Data Protection Officer

The reporter will be asked to provide the following information, or as much information is available. Reporting the breach should not be delayed whilst the information is collected.

- Nature of suspected breach including the types of data that have been compromised and how the potential data breach is believed to have occurred;
- Who is or may be affected including number of individuals;
- Consequences of the breach and what actions can be taken, or have been taken, to mitigate the breach.

Appendix 3

Flowchart showing notification requirements



Appendix 4

Information required to be recorded by the Data Protection Officer in the event of a Data Protection Breach

1. Personal data placed at risk
   a) What personal data has been placed at risk? Please specify if any financial or sensitive personal data has been affected and provide details of the extent.
   b) How many individuals have been affected and how many data records are involved?
   c) Are the affected individuals aware that the incident has occurred?
   d) What are the potential consequences and adverse effects on those individuals?
   e) Have any affected individuals complained to the University

2. Describe the incident in as much detail as possible.
   f) When did the incident happen?
   g) How did the incident happen?
   h) If there has been a delay in reporting the incident to the Data Protection Officer please explain the reasons for this.
   i) What measures were in place to prevent an incident of this nature occurring?
   j) Please provide extracts from any policies or procedures considered relevant to this incident, and explain which of these were in existence at the time of this incident. Please provide the dates on which they were implemented.

3. Containment and recovery
   k) Has any action been taken to minimise/mitigate the effect on the affected individuals? If so, please provide details.
   l) Has the data placed at risk now been recovered? If so, please provide details of ho and when this occurred.

   m) What steps have been taken to prevent a recurrent of this incident?

4. Miscellaneous
   n) Have the police or any other regulatory bodies been informed about this incident?
   o) Has there been any media coverage of the incident?

5. Data Protection Officer decisions
   p) Was the ICO informed of the breach? If not, what was the justification of not advising the ICO?
   q) Were the affected individuals advised of the breach? If not, what is the justification of not advising? If they were advised what advice was provided?