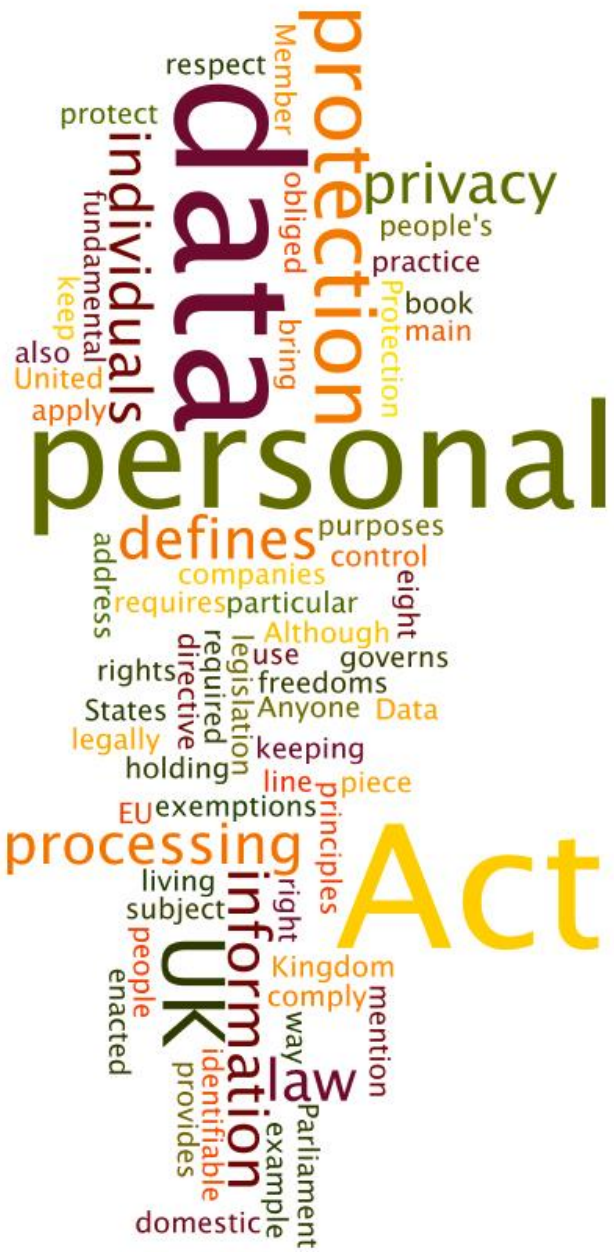
respect
protect
Member
protection
data
privacy
individuals
obliged
people's
practice
fundamental
keep
Protection
book
main
bring
also
United
apply
personal
defines
purposes
control
companies
address
requires
particular
eight
Although
use
governs
rights
directive
required
legislation
freedoms
States
Anyone
Data
legally
keeping
holding
line
piece
EU
exemptions
principles
processing
Act
living
right
subject
information
UK
Kingdom
people
comply
mention
enacted
way
law
identifiable
provides
Parliament
example
domestic

Information Security Incident Management Policy and Procedure

Revision History

Document	Information Security Incident Management Policy and Procedure
Author	Ty Walter
Date Completed	10 August 2009
Review Date	*August 2021*~~10 April 2015~~

Version	Revision Date	Revised By	Revisions Made
1.0	31 Dec 2008	Ty Walter	Original Document
1.1	06 Jan 2010	Ty Walter	Appendix 1 – 2.1 Procedure updated to include notifying GovCertUk.
1.2	12 Oct 2011	Ty Walter	Update to include reference to the Council's Digital Forensic Readiness Policy and minor updates to the 'reporting an incident procedure'.
1.3	23 Nov 2012	Ty Walter	Updated to include notifying PSN for any PSN security incidents categorised as 'major' or 'emergency'.
1.4	13 Feb 2015	Graham Leach	Updates to include the role & responsibilities of the Democratic Services Manager and Deputy Monitoring Officer in the process.
1.5	Feb 2018	Graham Leach/ Anna Moore	Updated to reflect new
1.6	*October 2019*	*Shafim Kauser*	*Update to reflect process for dealing with personal data breach*

Approvals
This document requires the following approvals:

Name	Title
Executive	5/4/2018

Distribution
This document has been distributed to:

Title

All Staff
All Members

Table of Contents

1 Management Summary

This policy is a constituent part of Warwick District Council's Information Governance Framework which sets out a framework of governance and accountability for information governance across the Council.

Safe use of the Council's information and IT systems is essential to keep it working effectively. All users of Council information have a responsibility to

- Minimise the risk of vital or confidential information being lost or falling into the hands of *unauthorised* people who do not have the right to see it
- Protect the security and integrity of IT systems on which vital or confidential information is held and processed
- Report *actual or* ~~suspected information~~ *suspected information* security incidents promptly so that appropriate action can be taken to minimise harm.

This document provides a framework for information security incident/event handling and response within Warwick District Council. Underpinning the Council's approach is the need to take prompt action in the event of any actual or suspected breaches of information security or confidentiality to avoid the risk of harm to individuals, damage to operational business and severe financial, legal and reputational costs to the organisation.

The General Data Protection Regulations (GDPR) introduce a duty on the Council to report certain types of information security incidents known as a personal data breach to the Information Commissioners Office (ICO) within 72 hours of becoming aware of the breach. Failure to notify a personal data breach when required to do so can result in a significant fine by the Information Commissioner of up to £10 million euros or 2 percent of global turnover.

This document outlines the steps to be taken when information security events *including personal data breaches* are discovered and establishes the organisational requirements, including roles and responsibilities for incident processing and protection. Using this document, incident handling and response can be performed in a consistent manner *and enables the Council to meet its duties to report an incident to the ICO where necessary*.

It is *therefore* essential that all information security events within Warwick District Council are reported **immediately** to the, ~~the~~ ICT Services Helpdesk or *in the case of a personal data breach, to the Information Governance Manager or* the Democratic Services Manager and Deputy Monitoring Officer.

Any member of Warwick District Council staff or contractors, who become aware of an Information Security Breach *(including a personal data breach),* or attempted breach of Warwick District Council systems, must report it immediately.

2 Policy Statement

All Warwick District Council staff, contractors and third parties, will report details of any information security incidents *including any personal data breach*~~or events~~, actual or suspected, related to the Council's paper or electronic information systems and data.

These information security weaknesses and events must be reported *immediately* ~~in a timely manner~~ through appropriate channels *allowing the Council to take necessary action and discharge its duties to report any personal data breach to the ICO where required*.

The Council requires commissioned services holding or processing information on its behalf to have in place internal reporting requirements equivalent to this procedure and for any third party breaches to be reported using this procedure.

3 Purpose

The purpose of this policy is to ensure that:

- all staff understand their roles in *identifying*, reporting and managing suspected incidents *in particular being able to quickly establish whether a security incident leads to a personal data breach*
  all actual or potential information security incidents are reported centrally to enable the Council to react quickly and effectively to minimise the impact.

The aims of the procedure are as follows:

- timely advice on containment and risk management
- investigate the incident and to determine whether further controls or actions are required
- evaluate lessons learnt and *identify* areas for improvement

The investigation should not be part of any disciplinary procedure that may take place subsequently.

4 Scope

This policy applies to:

- all Warwick District Council Councillors, employees (including temporary staff), contractors, sub-contractors and third parties with access to Warwick District Council information and information systems. Any reference in the document to "employee" or "staff" is deemed to include all of these groups of authorised users.
- all information created*,* ~~or~~ received *or processed* by the Council in any format, whether used in the workplace, stored on portable devices and media, transported from the workplace physically or electronically or accessed remotely

5 Definition

This policy needs to be applied as soon as information systems or data are suspected to be, or are actually affected by an adverse event which is likely to lead to a security incident.

An Information Security incident is defined as any event that has the potential to affect the Confidentiality, Integrity or Availability of Council Information in any format. *This includes a personal data breach which is defined as a security incident that affects the confidentiality, integrity or availability of personal data.* It may be a single or series of unwanted or unexpected information security events, *deliberate or accidental leading to the destruction, loss, alteration, unauthorised disclosure or access to* ~~that~~ *information. Information Security Incidents could* have a significant probability of causing harm to individuals, damage to operational business and severe financial, legal and reputational costs to the organisation. Some examples of possible incident categories include, but are not limited to:

- The disclosure of confidential information to unauthorised individuals
- Loss or theft of paper records, data or equipment such as tablets, laptops and smartphones on which data is stored
- Inappropriate access controls allowing unauthorised use of information
- Suspected breach of the IT and communications use policy
- Attempts to gain unauthorised access to computer systems, e, g hacking
- Records altered or deleted without authorisation by the data "owner"
- Virus or other security attack on IT equipment systems or networks
- "Blagging" offence where information is obtained by deception
- Breaches of physical security e.g. forcing of doors or windows into secure room or filing cabinet containing confidential information left unlocked in accessible area
- Leaving IT equipment unattended when logged-in to a user account without locking the screen to stop others accessing information.
- Covert or unauthorised recording of meetings and presentations
- Leaving confidential/personal information visible on desks without taking necessary precautions to protect while left unattended.
- *Loss of availability of personal data for example loss of access to personal account*

Any activities that violate this policy are considered an incident. Security incidents can be either accidental or deliberate.

5.1 Vulnerability

Vulnerability is where there is a known susceptibility within a specific product or service that could cause either a major or minor breach of Warwick District Council's Information Management Systems. Examples include:

- An inherent weakness in a core software module that opens applications to specific and potentially harmful exploits.
- Compromise of key services (e.g. web servers, DNS servers)

6 Applying the Policy

6.1 Roles and Responsibilities

6.1.1 All Users

Users are responsible for following the controls in place to protect the information they use and reporting any actual or potential breach of Information security promptly in line with the incident management procedure

6.1.2 Senior Information Risk Officer

The SIRO has overall responsibility for information as a strategic asset, ensuring that the value to the organisation is understood and recognised and that measures are in place to protect against risk. The Council's SIRO is the Deputy Chief Executive & Monitoring Officer.

6.1.3 Information Asset Owners

Heads of Service are also designated Information Asset Owners and are responsible for the management of information risk for their service's information assets. This includes ensuring that their information assets are properly recorded in the Council's information asset register.

6.1.4 Senior Managers

Senior managers are responsible for ~~identifying specific High and Medium risk information within their services and for~~ putting appropriate controls in place to minimise the risk of unauthorised access and the loss of data.

6.1.5 Data Protection Officer

The Council has appointed an Information Governance Manager who will act as Data Protection Officer for the Council. They are responsible for reporting on Data Protection compliance, advising on Privacy Impact Assessments for new systems and liaison with the Information Commissioner over data breaches, data protection notifications and other issues as appropriate.

6.1.6 System Owners

The responsibilities of the System Owner are fully defined in the Council's Information Security and Conduct Policy. In the context of this policy they are primarily responsible for:

- determining who can access the system and the scope of operation available to each permitted user as appropriate to the user's business needs;
- approving remote access connections from third parties, including the system supplier;
- removing users and associated access rights from the system when an employee leaves the organisation or changes job role and no longer requires access to the system;
- ensuring that a risk assessment is carried out on a new or replacement system, prior to going live;

- ensuring that the system is maintained in an effective and controlled manner;
- ensuring that all changes to the software are performed to an agreed change control mechanism;
- ensuring that staff immediately report any violations or misuse of the system to their line manager;
- ensuring that the sharing of information between internal departments, the public, suppliers, contractors and partners is in accordance with Council security policies and the Data Protection Act.

6.1.7 Deputy Chief Exec and Monitoring Officer (DCEMO)

The Deputy Chief Executive and Monitoring Officer has senior management accountability for information governance.

In the event of an suspected incident involving IT facilities, the DCEMO or his/her nominee is responsible for authorising the monitoring of a user's IT account, including use of computers, email and the internet in cases where this is necessary to investigate allegations of illegal activity or breaches of information security and for reporting such breaches, where relevant, to the relevant legal authorities.

6.1.8 Democratic Services Manager and Deputy Monitoring Officer (DSMMO)

The Democratic Services Manager and Deputy Monitoring Officer has senior management responsibility for the information governance and for providing proactive leadership to instil a culture of information governance within the Council through clear direction, demonstrated commitment, explicit assignment, and acknowledgment of information governance responsibilities.

6.1.9 ICT Services Manager

The ICT Services Manager is the lead officer responsible for ~~reporting~~investigating and taking appropriate action to address breaches of IT systems and network security, and for escalating incidents to the~~Information Security Officer~~*Data Protection Officer as appropriate*.

6.1.10 *Data Protection Officer (DPO)*~~Information Security Officer (ISO)~~

For the purposes of this policy the *Data Protection* ~~Information Security~~ Officer will be the *Information Governance Manager*~~Democratic Services Manager and Deputy Monitoring Officer~~. The *DPO*~~ISO~~ is the lead officer responsible for investigating and taking appropriate action in all cases involving loss, theft or unauthorised disclosure of Council *personal data*~~information~~ and for liaising with the other lead officers and Heads of Services in the management of other information security incidents. The ~~Information Security Officer~~ Data Protection Officer will record and review all information security incidents and make reports, as appropriate, to the ICT Steering Group*/Senior ManagementTeam*, recommending further action and any issues and risks to be escalated to the DCEMO and to the Council's Risk Management Group.

6.2 Information Security Incident Handling Procedure

Please refer to Appendix 1 for the Information Security Incident Handling Procedure

6.3 Reporting

All information security incidents whether actual or suspected, should be promptly reported to the ICT Services' Helpdesk and an individual's line or Service Area Manager. *In the case of a security incident involving personal data (personal data breach) the incident should be reported to the Information Governance* ~~or~~*Manager or* to the Democratic Services Manager and Deputy Monitoring Officer.

Even if an incident is not considered to be serious, it should always be reported as it may be part of a wider issue or trend *and helps the Council maintain a record of incidents*

6.4 Reporting of Software Malfunction

Users of information processing services are required to note and report any software that appears not to be functioning correctly (e.g. according to specification). They should report the matter directly to the ICT Services Helpdesk.

If it is suspected that the malfunction is due to a malicious piece of software (e.g. a computer virus) the user should:

- Note the symptoms and any messages appearing on the screen.
- Stop using the computer (isolate it if possible) and inform line management and notify the ICT Services Helpdesk immediately. If any investigations are to be performed on the machine it should be disconnected from the network before being switched back on again.
- Users should be informed that they should not, in any circumstances, attempt to remove the suspected software. All recovery action should only be undertaken by appropriately trained and authorised staff.

6.5 Incident Rating (See Appendix 2)

Incidents involving potential or actual data loss will be rated on a 1-5 scale when logged, but may be reclassified once the initial facts are determined. The description and examples are a guideline, but will be set by the ICT Steering Group.

Incidents at Level 3-5 are classed as a **Major Security Incident**.

A major incident is defined as a loss, potential loss, or breach of confidentiality of any information owned by WDC that is classified at the Confidential (Protect) or Restricted level, that will impact on WDC, an individual, or organisation.

~~Whilst there is no legal obligation in the Data Protection Act to report losses, the Information Commissioner's Office (ICO) consider serious breaches need reporting to them.~~

6.6 Information Security Response Team

Although the ICT Steering Group will be responsible for setting out the procedure for dealing with information security incidents in WDC, an Information Security Response Team will be responsible undertaking the investigations and making recommendations for action.

6.7 Standard Procedure for Investigations

For full details of the procedure for incident handling please refer to Appendix 1.

7 Policy Compliance

Any breach of this policy by staff may lead to disciplinary action being taken and, in cases of gross misconduct, termination of employment without notice. Some cases may result in the council informing the police and criminal action may follow. For Members, references in this policy to disciplinary action will be considered under the Arrangements for dealing with complaints about Councillors and this document will be treated as a local protocol for this purpose. Any breach of this policy by suppliers will be subject to appropriate action by the relevant Deputy Chief Executive.

Should the Council be sued due to misuse of Council ICT equipment or the actions of a user which contravene this policy, the Council reserves the right to claim damages from the authorised user concerned.

8 Policy Governance

The following table identifies who within Warwick District Council is Accountable, Responsible, Informed or Consulted with regards to this policy. The following definitions apply:

- **Accountable** – the person who has ultimate accountability and authority for the policy.
- **Responsible** – the person(s) responsible for developing and implementing the policy.
- **Consulted** – the person(s) or groups to be consulted prior to final policy implementation or amendment.
- **Informed** – the person(s) or groups to be informed after policy implementation or amendment.

Accountable	Deputy Chief Executive
Responsible	*Information Governance Manager*/ICT Services Manager / Democratic Services Manager and Deputy Monitoring Officer.
Consulted	SMT, ICT Manager, HR Manager

Informed	All Council personnel, temporary / agency staff, contractors, consultants, suppliers and Members.

9 Review & Revision

This policy will be reviewed as it is deemed appropriate, but no less frequently than every *2~~12~~* months.

Policy review will be undertaken by the Council's Information Governance Manager.

10 References

The following Warwick District Council documents are relevant to this policy:

- Warwick District Council - Digital Forensics Readiness Policy
- Warwick District Council – Data Handling Policy
- *Warwick District Council – Data Protection and Privacy Policy*

11 Key Messages

- All staff should report any incidents or suspected incidents immediately.
- ~~We can maintain your anonymity when reporting an incident if you wish. ????~~
- If you are unsure of anything in this policy you should ask for advice from ICT Services *or Information Governance Manager*.

Appendix 1 – Procedure for Incident Handling

1. Establishing an Information Security Response Team

Depending on the nature of the reported information security incident, the response will be led by either the Democratic Services Manager and Deputy Monitoring Officer (Information Governance) or the ICT Services Manager (ICT System Breach)

In the case of a personal data breach, the response will be led by the Information Governance Manager

In the event of a reported security incident, the response lead officer has the option of establishing an Information Security Response Team. The size and structure of this team will be appropriate to Warwick District Council and compromise key personnel from ICT Services, Human Resources, Property Services (Building Security) and Legal.

In addition to the above, where a major breach has occurred, specialist forensic services may be included within the team and the Police will be notified and/or included within the team if appropriate.

2. Reporting an Incident

2.1 Reporting

All information security incidents whether actual or suspected, should be promptly reported to the ICT Services' Helpdesk via an individual's line or Service Area Manager, or to the *Information Governance Manager/*Democratic Services Manager and Deputy Monitoring Officer *where the security incident involves personal data*.

2.2 Capture details

Establish the basic facts of the incident with the user/ service manager to give a provisional Incident Rating based on business risks and privacy. Use Appendix 2 (Incident Levels) for assistance.

- What happened
- When did it occur
- Who was involved
- What information assets were compromised/lost/disclosed/put at risk
- What security measures were in place
- What is the impact on individuals' privacy
- What is the impact on WDC, or others, business/services
- What immediate actions have been taken to minimise risk, recover any data loss *and*~~ain~~inform individuals/organisations affected

2.3 Record

Create an on-line Security Incident record within the Warwick District Council ICT Services Helpdesk system *or send the record to the Information Governance Manager/Democratic Services Manager*

2.4 Immediate Actions

The *Information Governance Manager*/Democratic Services Manager and Deputy Monitoring Officer or the ICT Services Manager will advise on any further actions that are required immediately to prevent further damage and facilitate initial recovery.

- Investigate the incident
    - Evidence Collection
    - *Contain the breach*
    - *Assess the potential adverse consequences*
    - *Carry out a risk assessment to establish the likelihood and severity of risk*
    - *Notify ICO within 72 hours of becoming aware of the personal data breach (if appropriate)*
    - *Notify individuals (if appropriate)*
    - *Notify a data controller (if appropriate)*
    - *Notify third parties such as insurers/banks (if appropriate)*
    - Notify GovCertUK (if appropriate)
    - Notify Police (if appropriate)
    - Immediately Inform the PSN Security Manager of all PSN Security Incidents with a PSN security severity level of 'Major' or 'Emergency'
- ~~Resolution identified~~
- ~~Resolution implemented (where applicable)~~
- ~~Report Produced~~
- ~~Appropriate documentation updated~~
- ~~Warwick District Council Management advised~~
- ~~Warwick District Council staff advised (e.g. procedural changes, additional training)~~
- ~~Legal Activity~~
    - ~~Civil~~
    - ~~Criminal~~
    - ~~Regulatory~~

~~In all cases, progress and outputs will be recorded within the security incident record held within the Warwick District Council helpdesk system.~~

3. Security Incident Investigation

When a security incident is reported or received by the ICT Services Helpdesk/*Information Governance Manager or Democratic Services Manager and Deputy Monitoring Officer*, a decision will be made by either the *Information Governance Manager*/Democratic Services Manager and Deputy Monitoring Officer or the ICT Services Manager as to whether an investigation into the incident will be carried out and who will be tasked to carry out the investigation. This may also involve establishing an Information Security Response Team where a major incident has occurred.

All investigations will be treated in confidence and disclosure only made when authorised by the Democratic Services Manager and Deputy Monitoring Officer or the ICT Services Manager.

The investigation will identify:

- When, how and who discovered the breach
- What happened
- What were the reasons for the actions that led to the incident
- Who was involved
- What information assets were compromised/lost/disclosed/put at risk
- What security measures were in place
- What is the potential impact on an individuals' privacy
- Who has been notified so far
- What is the potential impact
- Is there media interest and/or complaints
- What remedial actions are already underway
- What areas of improvement, organisational issues or training needs can be identified.
- if any person is culpable and whether disciplinary action is necessary.

If the incident level is major or, as a result of the investigation, the incident has been reclassified as major then the Information Security Response Team will need to consider if the incident should be reported to:

- GovCertUK (if appropriate)
- the Police (if appropriate)
- the ICO
- the PSN Security Manager for all PSN Security Incidents with a PSN security severity level of 'Major' or 'Emergency'

4. Security Investigation Records

For all Warwick District Council investigations, an investigation record must be maintained throughout the conduct of the investigation and the resolution of the breach. All investigations will be classified as Restricted and handled accordingly.

5. Collection of Evidence

5.1 Paper Documents

Any paper information retained as evidence must be kept securely, with a record of the individual who found the document, where the document was found, when it was found and who witnessed the discovery. This information must be recorded in the investigation log. Any original documentation retained, as evidence, must not be tampered with.

5.2 Information Held Electronically

For further information please refer to the Council's Digital Forensics Readiness Policy and ACPO's Good Practice Guide for Computer-Based Electronic Evidence

6. Report and Retention

~~On completion of every investigation, an investigation report is to be submitted by the investigator to the ICT Steering Group and held centrally in a secure repository and retained for a period of 36 months from the date of report being completed.~~*On completion of every investigation, an investigation report is to be submitted by the investigator to the ICT Steering Group/SMT and held centrally in a secure repository and retained for the period defined in the Council's retention policy.*

7. Learning from Incidents

Once an information security incident has been closed, it is important that the lessons learned from the handling of the information security incident are quickly identified and acted upon. This could include:

- Implementation of additional controls (physical, technical or procedural)
- Raising security awareness
- Changes to the information security incident management process
- *Providing additional training*

Information contained within the information security incident database should be analysed on a regular basis in order to:

- Identify trends/patterns
- Identify areas of concern
- Analyse where preventative action could be taken to reduce the likelihood of future incidents.

8. Identification of Security Improvements

During the review process of a security incident, additional controls may need to be implemented by Warwick District Council. The recommendations and related additional controls may not be feasible (financially or operationally) to implement immediately, in which case a Risk Assessment should be conducted and the actions added to the appropriate services Risk Log.

Appendix 2 – Incident Levels

Level	Incident Type	Description	Notifications Internal	Notifications External
1	Minor	No loss, policy/process followed e.g. lost encrypted laptop/iPad		
2	Moderate	No loss or possible minor loss, low risk and impact to individual, but policy/process not followed or previous incidents. **Examples**; email policy breach, laptop not encrypted but only public data stored.		
3	Major	Temporary loss of personal data or council confidential (Protect) data, medium risk potential impact on individuals or organisations. Policy/process followed, data recovered or secured. **Examples**; letter lost, letters/emails sent in error to wrong recipients.		
4	Major	Personal or confidential (Protect) business data breach. Policy process not followed, data recovered. Consider impact and if a 'serious' breach of data under DPA for reporting to ICO. **Examples**; correspondence and assessment lost or sent to wrong recipient, unencrypted device with minor personal data.		
5	Major	Data breach for sensitive personal data or Restricted data for a person, business or a number of people. Data not located or recovered. Consider impact and if a 'serious' breach of data under DPA for reporting to ICO. **Examples**; benefit claim information, including health and financial information lost, significant volumes of customer data lost/released into the public domain, confidential waste lost, health related data sent to wrong address/email, unencrypted device with sensitive personal data. **Further Examples;**		

		Information that could be used to commit identity fraud such as personal bank account and other financial information and national identifiers, such as national insurance numbers and copies of passports and visas Personal information relating to vulnerable adults and children Detailed profiles of individuals; including information about work performance, salaries or personal life that would cause significant damage or distress to that person if disclosed Sensitive negotiations which could adversely affect individuals. Security information that would compromise the safety of individuals if disclosed. Information received in confidence .e.g. legal advice from solicitors, trade secrets and other proprietary information received from contractors, suppliers and partners Information that would substantially prejudice the University or another party's intellectual property rights, commercial interests or competitive edge if it were disclosed Information relating to high profile/high impact strategy or policy development before the outcomes have been decided and announced. Information that would compromise the security of buildings, equipment or assets if disclosed.		

Notifications Key

For PSN purposes a major breach is a Security Incident with a PSN security severity level of 'Major' or 'Emergency';

Emergency	An incident that the service users should be aware of, and may have a significant impact to the service as: they have specific core or widespread use of the vulnerable technology **or** the vulnerable technology is security enforcing for part, or all of the system, service, or infrastructure **and** the exploitation of the vulnerability may be possible either locally and/or remotely the exploitation would likely lead to high / very high impact to the service, users, or PSN infrastructure.
Major	An incident that users should be aware of, and may have a detrimental impact to the service as: they have specific core or widespread use of the vulnerable technology **and** the exploitation of the vulnerability may be possible either locally and/or remotely the exploitation would likely lead to a medium / high impact to the service, users, or PSN infrastructure.

Appendix 1 – IS Incident Handling Procedure

1. Incident Notification

- All information security incidents whether actual or suspected, should be promptly reported to the ICT Services' Helpdesk, or *in the case of a personal data breach to the Information Governance Manager*/~~to the~~ Democratic Services Manager and Deputy Monitoring Officer (DSMDM) *by completing the attached Incident Log (Appendix 3).*
- Incident reporting requires the notifying officer to provide key details of the incident including:
  - ✓ What happened
  - ✓ When did it occur
  - ✓ Who was involved
  - ✓ What information assets were compromised/lost/disclosed/put at risk
  - ✓ What security measures were in place
  - ✓ What is the impact on individuals' privacy
  - ✓ What is the impact on WDC, or others, business/services
  - ✓ What immediate actions have been taken to minimise risk, recover any data loss and inform individuals/organisations affected
- Once the Incident has been reported it will be logged centrally by the ICT Helpdesk *or the Information Governance Manager*.
- **Important:** In the event of a Cyber security Incident, the ICT Services Manager or any ICT staff member may invoke the Major Outbreak Virus Procedure. This procedure is designed to prevent further damage and facilitate initial recovery. This may include:
  - ✓ Immediate disconnection of the Council's corporate Internet connection
  - ✓ Disconnection of server network adaptors

2. Incident Assessment

- The *likelihood and* severity of an incident will be determined by the incident rating – See Appendix 2
- Upon notification an initial assessment of risk will be undertaken by the *DPO*/DSMDM or ICT Services Manager to determine a provisional incident rating and appropriate notifications will be made as per the applicable rating.
- An incident rating may change once the full facts and impact of risks has been determined and the status of the incident will be kept under review accordingly.

3. Incident Investigation

- Not all incidents will require an in depth investigation to establish the facts and determine what went wrong. This will often depend on the level of detail provided when the incident was reported, *the nature of the incident and any action already taken*.
- If any additional information is required then the Incident Lead will contact the notifying officer or any other persons involved in the incident to seek clarification or further information.
- Any incidents rated as medium or high risk may require a full scale investigation by the Incident Lead:
  - ✓ **Breaches of ICT Security:** ICT Services Manager
  - ✓ **Breaches of Information Security:** *Information Governance Manager*/Democratic Services Manager and Deputy Monitoring Officer
  - ✓ **Breaches of Physical Security:** Building Manager
- At the conclusion of the investigation the Incident Log should be ~~completed and/or~~ updated.- See Appendix 3

4. Incident Review

- The *Incident Lead will review the Incident and carry out a risk assessment* ~~completed Incident Log will be produced within 5-10 days~~ setting out:
  - ✓ observations and conclusions about any information governance non-compliance issues, risks, adverse consequences or implications
  - ✓ remedial recommendations to mitigate the risks and impact including preventative measures to address areas for improvement and training needs.
- Any repeat or previous similar incidents will be flagged and may result in additional or escalated action.
- The final Incident Log *and risk assessment* will be *retained by the* ~~sent to the~~*DPO/*DSMDM/*ICT Services Manager* and/or the Deputy Chief Executive and Monitoring Officer. *This may* ~~to sign off and accept~~*set out* ~~the~~ recommendations *and*~~by~~ appoint~~ing~~ a responsible officer and target dates for implementation.
- It ~~*may*will also~~ *may also* be shared with other key staff or specialist teams in accordance with the incident rating.
- This procedure is independent of any disciplinary investigation but the final Incident Log *and risk assessment* may inform any consequential action taken or considered.

5. Incident Monitoring & Closure

- The responsible officer will be required to update an Incident Log to indicate when recommended action has been implemented by completing the 'actions taken' and 'date action complete' fields.
- If appropriate, the *DPO*/DSMDM and /or the ICT Services Manager shall report to the ICT Steering Group (ICTSG) with any recommendations for changes to corporate policies, procedures and training including lessons learnt
- An incident will only be closed when all recommendations have been completed.

Appendix 3 – Incident Log

Type of Incident	Please Tick
ICT Security	
Information Security	
Physical Security	

Initial Log	
Date and time of Incident	
Who reported the Incident?	
Who was involved in the Incident.? Member, Officer, 3rd Party	
Was personal / sensitive data involved?	
If yes to the above, how many records were involved?	
Summary of the actual or suspected security breach	
What immediate actions have been taken to minimise risk, recover any data loss and inform individuals/organisations affected	

- ✓ What information assets were compromised/lost/disclosed/put at risk
- ✓ What security measures were in place
- ✓ What is the impact on individuals' privacy
- ✓ What is the impact on WDC, or others, business/services
- ✓ What immediate actions have been taken to minimise risk, recover any data loss and inform individuals/organisations affected
- When, how and who discovered the breach

- What happened
- What were the reasons for the actions that led to the incident
- Who was involved
- What information assets were compromised/lost/disclosed/put at risk
- What security measures were in place
- What is the potential impact on an individuals' privacy
- Who has been notified so far
- What is the potential impact
- Is there media interest and/or complaints
- What remedial actions are already underway
- What areas of improvement, organisational issues or training needs can be identified.
- if any person is culpable and whether disciplinary action is necessary.

Appendix 4 – Examples of Incidents and Possible responses

Level	Incident Type	Description	Possible response
1	Minor	No loss, policy/process followed e.g. lost encrypted laptop/iPad	Record note, consider learning opportunities and feedback for staff.
2	Moderate	No loss or possible minor loss, low risk and impact to individual, but policy/process not followed or previous incidents. **Examples**; email policy breach, laptop not encrypted but only public data stored.	Example could be a general email or letter going to the wrong individual. For example notification of public consultation starting. Note the issues and consider future mitigations, remind staff of appropriate procedures that are in place.-
3	Major	Temporary loss of personal data or council confidential (Protect) data, medium risk potential impact on individuals or organisations. Policy/process followed, data recovered or secured. **Examples**; letter lost, letters/emails sent in error to wrong recipients.	Sending the response to a complaint or about personal service to the incorrect recipient but the letter is returned to

			the Council or it is confirmed email deleted and not opened. Remind staff about correct procedure and record to look for patterns of behaviour or breaches. Potential review of how information is despatched to look for ways to remove human error.
4	Major	Personal or confidential (Protect) business data breach. Policy process not followed, data recovered. Consider impact and if a 'serious' breach of data under DPA for reporting to ICO. **Examples**; correspondence and assessment lost or sent to wrong recipient, unencrypted device with minor personal data.	An example could be an email sent to a mailing house, via an unsecure method, with contact details for mailing to be sent to individuals. However email blocked from sending by IT due to content restriction filter. Remind staff of process and no need to inform effected customers. However if released and sent to

			incorrect address then there would be a need to notify ICO, consider action and notify all customers who's data was released.
5	Major	Data breach for sensitive personal data or Restricted data for a person, business or a number of people. Data not located or recovered. Consider impact and if a 'serious' breach of data under DPA for reporting to ICO. **Examples**; benefit claim information, including health and financial information lost, significant volumes of customer data lost/released into the public domain, confidential waste lost, health related data sent to wrong address/email, unencrypted device with sensitive personal data. **Further Examples;** Information that could be used to commit identity fraud such as personal bank account and other financial information and national identifiers, such as national insurance numbers and copies of passports and visas Personal information relating to vulnerable adults and children Detailed profiles of individuals; including information about work performance, salaries or personal life that would cause significant damage or distress to that person if disclosed Sensitive negotiations which could adversely affect individuals. Security information that would compromise the safety of individuals if disclosed.	For example loss of a personal file in a public domain such as housing tenancy file, personnel file complaint file, disciplinary file or subject access request. There would be a need to notify the individual of potential loss once identified, carry out reasonable searches to identify location of material and provide reassurance. LAso notify the ICO expecting a full audit by them of practice and behaviours. Potential actions against staff if not following policy.

		Information received in confidence .e.g. legal advice from solicitors, trade secrets and other proprietary information received from contractors, suppliers and partners Information that would substantially prejudice the University or another party's intellectual property rights, commercial interests or competitive edge if it were disclosed Information relating to high profile/high impact strategy or policy development before the outcomes have been decided and announced. Information that would compromise the security of buildings, equipment or assets if disclosed.	