Section 1 – Data Protection and Security Incident Reporting Policy

1. Policy Introduction

1.1 The information the Council holds, processes, maintains and shares with other public sector organisations is an important asset that, like other important business assets, needs to be suitably managed and protected.

1.2 In order to build public confidence and ensure the Council complies with relevant legislation, it is vital to maintain the highest standards of information security.

2. Policy Statement

2.1 The Council (as Controller) recognises that security incidents can lead to the loss of Council and/or Personal Data. If not addressed in an appropriate and timely manner a security incident can result in a Personal Data Breach. This loss can lead to physical, material or non-material damage to individuals such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of Pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the individual concerned.

2.2 Where a security incident and/or Personal Data Breaches does occur the Council will, without undue delay, seek to contain the harm to the Council and individuals, investigate the incident, and look to learn the lessons from any actual or suspected security incident or Data Protection Breach at take remedial action. Also, where required by the current Data Protection Legislation, the Data Protection Breach will be reported to the Information Commissioner's Office (ICO) within 72 hours.

3. Purpose

3.1 The aim of this policy is to ensure that the Council reacts appropriately to any actual or suspected security incident and/or Personal Data Breaches.

4. Scope

4.1 This document applies when a Security Incident and/or Personal Data Breach is suspected. This policy and procedure shall be followed by:

- All permanent employees
- All temporary/contract employees employed or engaged by the Council
- Workers/volunteers employed or engaged by the Council
- All employees of partner or subsidiary organisations whilst at work and/or engaged on Council business;
- Councillors
- Any other authorised user

4.2 This Policy should be applied with appropriate reference to the Council's Data Protection Policy and the Information Security Policy.

5. Definitions

Personal Data - means any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier

Personal Data Breach - means a breach of security leading to or which is likely to lead to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise processed. A Personal Data Breach includes, but is not restricted to, the following:

- The accidental alteration or deletion of personal data;
- The transfer of personal data to those who are not entitled to receive it;
- Unauthorised access to personal data;
- Use of personal data for purposes for which it has not been collected and which go beyond those uses that the data subject could reasonably have contemplated; and
- Theft of storage devices

Pseudonymisation - means the processing of personal data in such a way that the personal data can no longer be attributed to a specific data subject (giving them a pseudonym) without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to that data subject without authorisation;

Data Subject - means the person who the Personal Data is about

Data Protection Legislation - means The General Data Protection Regulation 2016 the Law Enforcement Directive 2016, The Data Protection Act and all applicable Laws relating to Personal Data and privacy

Security Incident - means the actual or potential accidental, deliberate or unlawful destruction, loss, alteration, unauthorised disclosure of, corruption or access to, personal data or Council information or the theft, loss or damage to Council IT equipment including mobile phones and handheld devices

ICO - means the Information Commissioner

6. Roles and Responsibilities

Senior Information Risk Owner (SIRO) - ensures information assets and risks within the Council are managed as a business, actively work with the Data Protection Officer and other experts within or outside the Council to determine the most effective and proportionate information control measure. The SIRO is responsible for building an informed culture within the Council to promote the best practice for the use and protection of Information assets. The SIRO is responsible for implementing current Data Protection Legislation on behalf of the Council (the Controller).

Single Point Of Contact For Controller (SPoC) - acts as single point of contact for customers, staff and the Data Protection Officer in relation to Personal Data. Support the SIRO in ensuring the Council can demonstrate compliance with current Data Protection Legislation.

Data Protection Officer (DPO) - undertakes the statutory role by monitoring compliance and by providing advice and assistance to the SIRO. The DPO may report directly to the Council's Executive Leadership Team and shall provide training on policies relating to data protection. One Legal provides day to day legal advice and assistance on Data Protection Legislation.

Information Asset Owners (IAO) - are the Service managers responsible for ensuring that their service areas comply and can demonstrate compliance with current Data Protection Legislation.

Staff - all staff are responsible for ensuring that the Personal Data they handle is processed in accordance with this Policy and current Data Protection Legislation

IT Manager - lead officer for ICT security

7. Risks

7.1 The Council recognises that there are risks associated with the collection, use, transmission and storage of data including Personal Data in order to conduct official Council business. By following this policy and procedure, suspected Security Incident and/or Personal Data Breaches should be identified quickly and the impact of Security Incident and/or Personal Data Breaches should be reduced by ensuring suspected Security Incident and/or Personal Data Breaches are followed up correctly, and helping identify areas for improvement.

8. Procedures for Reporting Data Protection and Security Incidents

8.1 Following an investigation as set out in Section 2 the IAO in consultation with the SPoC and One Legal will make an assessment of risks.

8.2 Where any risk is classed as 'High' the IAO or SPoC will advise the SIRO who will seek advice from the DPO and:

- If the SIRO in consultation with the DPO concludes that the Personal Data Breach is likely to result in a high risk to the rights and freedoms of the Data Subject, the SPoC will notify the Data Subject and the ICO directly.
- The SIRO in consultation with the DPO will agree what measures should be taken to deal with the Security Incident and/or Personal Data Breach and any changes to the way the council and/or Personal Data is processed in the future.
- The SIRO will inform the Council's Senior Management Team as soon as possible after receiving a report of a Security Incident and/or Personal Data Breach of the result of the investigation and the action to be taken.
- In the event that it is not possible to report the Personal Data Breach to the ICO within 72 hours, the notification will also give the reasons for the failure to do so.
- The DPO will act as the point of contact for the ICO and the SPoC will assist the DPO in providing information to the ICO.

9. Review and Revision

9.1 This policy and procedure will be reviewed by the SIRO in consultation with the DPO as it is deemed appropriate, but no less frequently than every 12 months.

Section 2 - Data Protection and Security Incident Response Plan and Reporting Process

The purpose of the Security Incident/Data Protection Breach Response Plan is to outline the investigation, considerations and actions to inform an appropriate response to a suspected or actual Security Incident and/or Personal Data Breach.

1. Definition and Types of Data Protection and Security Incidents

1.1 This Data Protection/Security Incident Response Plan relates to both electronic and paper copies of information held by the Council or organisation that process data including Personal Data on behalf of the Council.

1.2 There are numerous types of Incident including:

- Unauthorised disclosure of protected / exempt information
- Computer infected by virus or other malware
- Disclosing of personal data to unauthorised persons or organisations
- Loss of paper files containing personal or sensitive data
- Unauthorised access to restricted data which results in loss or corruption of data
- Receiving and forwarding chain emails
- Social engineering and Phishing, ransomware, spyware activity to obtain data
- Criminal damage to council equipment holding data
- Web site defacement (unauthorised link attachments)
- Use of unapproved or unauthorised software on Council equipment
- Connecting unauthorised devices to the council network
- Printing or copying official sensitive information and not storing it correctly
- A breach of the Council's information security policy, or sub policies by an employee, contractor or Councillor.
- Sending an email containing Personal Data to the wrong person
- Receiving unsolicited mail of an offensive nature e.g. containing pornographic, obscene, racist, sexist or grossly offensive or violent material.
- Receiving unsolicited mail which requires you to enter Personal Data
- Theft, insecure disposal or accidental loss of written or electronic data or of any Council equipment holding restricted data.

2. Initial Response and Reporting a Data Protection and/or Security Incident

2.1 For all types of Data Protection and Security Incidents Staff and Members are required to report concerns immediately to the relevant IAO.

2.2 The IAO will inform the SPoC and take immediate remedial action to contain the incident/breach. Appropriate action will also be taken to retrieve any Personal Data and/or prevent destruction, loss, alteration, unauthorised disclosure of, corruption or access to, personal data or Council information.

2.2 The IAO should complete the Data Protection and Security Incident Reporting Form with the assistance of the SPoC and confirm the details of the incident. If the SPoC is not available, please contact the SIRO or in their absence One Legal.

2.3 The IAO, in consultation with the SPoC and One Legal, should apply the initial risk assessment to grade the severity of the incident and then establish the appropriate response team (see point 3).

2.4 Where the risk assessment is classed as 'High', the IAO or the SPoC shall refer the incident to the SIRO who will seek advice from the DPO.

2.5 Where the risk assessment is classified 'medium' the IAO will lead the response in conjunction with those people listed in the table below, The SPoC will seek advice from One Legal

2.6 For 'Low' assessments the SPoC will seek advice from One Legal. Once that advice is considered by IAO and the SPoC, the SPoC will forward the finalised Data Protection and Security Incident Reporting Form to One Legal.

2.7 One Legal will forward the form to the DPO for sign off.

3. Investigation

3.1 Response teams and reporting arrangements

- Based on the severity rating for the incident, an incident response team will need to be established by the IAO and SPoC as described below.
- The lead officer will be SIRO for high risk incidents, and the IAO for low and medium risk incidents.
- An investigation plan should be agreed with the team and sufficient resources will need to be identified for the team to conduct the preliminary investigation, and any follow up investigation and reporting.

Initial Risk Assessment	Summary of internal response and reporting requirements	External Reporting
Low Risk	• IAO led response team with SPoC and IT support if necessary • Seek advice from One Legal	n/a
Medium Risk	• IAO led response team SPoC and IT support if necessary • Possible Internal audit involvement in the investigation and reporting process depending on the number of records affected and nature of incident. • Seek advice from One Legal	Warning, Advice and Reporting Point (WARP) - ICT Manager to action
High risk	• SIRO led response team reporting to the Chief Executive • Seek advice from One Legal • HR involved if there are allegations of staff misuse and/or a breach of the code of conduct • External communications plan needed • Internal audit and DPO involvement in the full investigation process.	ICO – SIRO & DPO to action Warning, Advice and Reporting Point (WARP) - ICT Manager to action

3.2 Accountability, reporting and progression

The SIRO in consultation with the DPO is responsible for recommending further action to the Senior Management Team and the IAO.

3.3 Corrective work: systems

If there have been problems which are caused by system failures, these should become apparent as the initial investigation unfolds. Where there is an immediate solution in order to prevent further loss of information, this should be recommended and immediate action taken.

4. Disciplinary Action

4.1 Once the preliminary investigation has been completed the IAO should contact HR if there is any evidence that disciplinary action may be necessary.

5. Post Investigation and Follow Up

5.1 The SPoC will monitor the Data Protection/ Security Incident Log to ensure the Council is continuing to comply with Data Protection Policy and the Information Security Policy, and the security incidents are being dealt with in a proper and timely manner.

5.2 The SpoC shall ensure the IAO's implement any changes required to protect data in the future.

6. Communication

6.1 Communicating to customers, Members, partners and stakeholders, the SPoC must consult with the SIRO, and, where appropriate, DPO regarding all communication with customers affected by the Security Incident and/or Personal Data Breach

6.2 For all high risk incidents, the SPoC must draw up a communication plan to ensure;

- all adversely affected parties are kept informed of the Council's investigation of the incident
- appropriate action is taken to prevent any further incidents
- action is taken to manage the immediate impact of the incident on customers or stakeholders whose information may be at risk or whose connection to the network or business systems may be disrupted.

7. Media Response Plan

7.1 The SPoC is responsible for liaising with the communications team to prepare a media response plan where necessary. The plan should provide reassurance on any public interest issues and promote any help lines for members of the public who may be adversely affected by the incident.

8. National and Regional Security Networks

8.1 The are two main security networks which monitor IT security incidents, which the Council are obliged to report an incident to, depending on the risk assessment of that incident.

GovCert UK: Is the Computer Emergency Response Team (CERT) for UK Government. They assist public sector organisations in response to ICT security incidents and can assist the organisations to effectively recover from and prevent the reoccurrence of network security failures. Information about GovCert UK can be found at http://www.govcertuk.gov.uk.

DWP LASST: Department for Work and Pensions, Local Authority Security & Support Team have established guidance on the reporting of security incidents affecting Housing Benefit Official

Sensitive data. There are prescribed procedures for information security, which include advising LASST immediately if it becomes aware of any actual or suspected security breach involving DWP data. This should be done by contacting their security team on the following email address HBSDSECURITY.TEAM@DWP.GSI.GOV.UK

Other useful networks which can be provide benefits to member organisations who contribute security incident information are:

WARPS: Warning, Advice and Reporting Point – these are forums organised regionally as a means of sharing information and alerting member organisations of current or possible threats to information security. It is intended to be a proactive and preventative network which members can contribute to anonymously, for the benefit of all members.

9. Linked Procedures, Policies and Statute

9.1 Breach of Confidentiality:

- Code of Conduct for Employees - leading to possible disciplinary action
- Members Code of Conduct, reported to the Council's Monitoring Officer.
- Council's whistle policy
- Data Protection policy – the council's Data Protection Policy requires the Council to manage personal data appropriately, both protecting it from unnecessary loss or misuse, whilst also meeting requirements for data sharing and public access when appropriate.
- Computer Misuse Act 1990 – defines offences related to unauthorised access to software, services or data.
- Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR) relates to direct marketing by electronic means and the use of cookies.
- Data Protection Legislation

Section 3 – Data Protection and Security Incident Reporting Form

To be completed by the IAO and forwarded to SPoC, with a copy retained by the SIRO.

Your Details:

Name and contact details	
Job Title / Team	
Date reported	
Please tick box to confirm you have read: Section 1 - Data protection & information security policy Section 2 - Data protection & security incident response plan & reporting process	

2. Details of the Security Incident / Data Protection Breach:

Details of Incident

Date, time and location of the incident.	
How did you find out about the incident?	
Provide a full description of the incident setting out the actions you have taken	
Information of Gloucester city council employees held on external source. Data did not include name or address but did include post code and asked questions about how they travelled to work	

Type of Data

What type of data is involved? e.g. does it include, name, address, telephone number, email address	
Is the Personal Data classed as Special Categories of Personal Data? (Information relating to the racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.)	
Is the data publically available elsewhere? E.g. check on – line/search engines, 192	

Risk to the Data Subjects

How has the incident been contained? e.g. has the data been returned, has the recipient confirmed that it has been destroyed/deleted (get written confirmation), has the data been taken offline?	

Is the Personal Data in a form that could be easily replicated or passed onto other third parties?	
Is the Personal Data in a form that could be copied and misused i.e. electronic signatures?	
What harm could come to those individuals? Could they suffer financial loss, reputational risks, risk to their physical safety? Please state if there has been any actual harm to the data subject.	

IT Security Incident

The asset number of any IT equipment affected (laptops, digital cameras, mobile phones, hand held devices)	
Did the incident lead to or was likely to lead to the theft, loss or damage to Council IT equipment including laptops, mobile phones and handheld devices	
Did the incident involve or was likely to involve a hacking or ransomware, spyware or unauthorised access to the Council's IT system? Give details of how access was gained and what systems have been accessed.	
What action has been taken to secure the council's IT system?	
Did the incident lead to or is likely to lead to the actual or potential accidental, deliberate or unlawful destruction, loss, alteration, unauthorised disclosure of, corruption or access to, personal data or council information?.	

Mitigating Loss & Future Learning

Describe the steps taken to limit the loss in this incident	
Describe the steps taken to prevent or limit the likelihood of a similar incident happening again (e.g. training, double checking post)	

3. Initial Assessment of Risk

RISK NO.	RISK		TICK
1.	LOW	Unrestricted data is *of little* public interest and would not result in a risk to the rights and freedoms of individuals or damage to the council's reputation	
		For Personal Data: Breach *unlikely* to result in a risk to the rights and freedoms of an individual	
	MEDIUM	Data which have *significant local interest a*nd incident would damage the council's reputation in the short/medium term contains	
		For Personal Data: Breach *may* result in a risk to the rights and freedoms of an individual	
	HIGH	Data is of *high interest locally and nationally*. Distribution/publication of data could result in critical longer term damage to the council's reputation.	
		Large amounts of Personal Data and/ or Special Categories of Personal Data involved in breach.	
		For Personal Data: Breach is *likely* to result in a risk to the rights and freedoms of individuals	
2.	LOW	Volume of records less than 10	
	MEDUIM	Volume of records 10 to 50	
	HIGH	Volume of records 50 plus	
3.	LOW	Password protected and encrypted – very difficult to access and use	
	MEDIUM	Password protected-some protection	
	HIGH	No protection	
4.	LOW	Little risk of further loss as a result of the incident	
	MEDIUM	May risk further loss as a result of the incident	
	HIGH	Likely risk of further loss as a result of the incident	
5.	LOW	Unlikely risk of claims or other action against the council as a result of data loss or corruption	
	MEDIUM	May be risk claims or other action against the council as a result of data loss or corruption	
	HIGH	Likely risk of claims or other action against the council as a result of data loss or corruption	
6.	LOW	No major disruption to services against the council	
	MEDIUM	Short term disruption, with some catch up required to restore business as usual service	
	HIGH	Loss of data will cause major disruption to delivery of a critical service, with no planned back up procedure	

4. Initial Assessment of Risk

Overall Risk Assessment Level	
Reason for risk level	

For any medium and high risks identified please complete parts 6, 7 and 8.

For low risk assessments please just complete part 5.

5. Signatories for Low Risk Incidents

IAO Name & Job Title	
Signature	
Date	

SPoC - Name	
Signature	
Date	

6. Assessment of Risks for Medium and High Incidents

For medium and high risks please provide further information about each medium or high risk, as identified above, and assess the outcome level of risk after taking into account any solutions.

Risk No	Initial Risk Level	Solution/Assessment	Result of Solution/Assessment (resolved, reduced or unresolved)	Post Solution Risk Level
1				
2				
3				
4				
5				
6				

7. Signatories and Record of Outcomes for Medium & High Risk Incidents

Risk No.	Approved by: Information Asset Owner (low or medium) and SIRO(high)	Name/Date
1		
2		
3		
4		
5		
6		

Advice of DPO (for High):	
Summary of DPO advice:	
If you have not accepted the advice of the DPO please provide your reason:	

5. Signatories for Medium and High Risk

IAO Name & Job Title	
Signature	
Date	

SPoC - Name	
Signature	
Date	

SIRO - Name	
Signature	
Date	

8. Post Investigation and Follow Up
