PSN (GCSx) Acceptable Usage Policy.

Signed: **Chief Executive.**

Document Control

Organisation	Dacorum Borough Council
Title	PSN / (GCSx) Acceptable Usage policy
Author	John Worts
Filename	DBC070 IS Policy – PSN / (GCSx) Acceptable Usage Policy.
Owner	
Subject	
Protective Marking	None
Review date	5th August 2019

Contents

1 Policy Statement

It is Dacorum Borough Council policy that all users of PSN / (GCSx) understand and comply with corporate commitments and information security measures associated with PSN

Please note that due to government framework contracts, the use of PSN may change over time. This Policy will be updated to reflect such changes.

2 Purpose

PSN – Stands for Public Sector Network, GCSx stands for Government Connect Secure Extranet. It is a secure private Wide-Area Network (WAN) which enables secure interactions between connected Local Authorities and organisations.

Some Council staff will be required to have access to the facilities operated on this network in order for them to carry out their business. This may include staff having access to government gateways or portals. All staff requiring access to the PSN network in any way will be required to read and understand this Acceptable Usage Policy (AUP) and sign the Personal Commitment Statement.

3 Scope

All users of the PSN / (GCSx) connection must be aware of the commitments and security measures surrounding the use of this network.

3.1 This policy applies to all councillors, employees, partners, contractors and agents of the Council (i.e. voluntary sector) who use or have access to the PSN network, computer equipment or ICT facilities.

3.2 IT Hardware includes, but is not limited to: desktop PCs, Laptops, Tablet devices, network cabling, routers, firewalls, switches, hubs, mobile phones, smartphones, printers, removable storage devices, digital cameras and other peripheral devices, owned by the Council or 3rd Parties.

3.3 IT Software includes, but is not limited to: operating systems and applications running on any of the above hardware, web applications and solutions hosted either internally or by 3rd parties.

4 Policy Compliance and Disciplinary Action

4.1 All employees, councillors and anyone who delivers services on the Council's behalf e.g. contractors, partners, agents or other third parties with access to the Council's information assets have a responsibility to promptly report any suspected, potential or observed security breach;

4.2 ALL BREACHES MUST BE REPORTED TO THE COUNCIL'S INFORMATION SECURITY OFFICER IN THE FIRST INSTANCE – FURTHER DETAILS ARE PROVIDED IN THE '**Personal Data Breach or Incident Reporting Procedure**' (DBC999 IS Proc) found on the Council's Intranet.

4.3 Security breaches that result from a deliberate act or omission or from an otherwise negligent disregard of any of the Council's security policies and/or procedures may result in disciplinary

action being taken against the employee under their contract of employment or, in the case of a councillor, under the Members' Code of Conduct. In the event that breaches arise from a deliberate or negligent disregard for the Council's polices and/or procedures, by a user who is not a direct employee of the Council, or a councillor, the Council may take such punitive action against that user and/or their employer as the Council deems appropriate.

4.4 The Council may refer the matter of any breach of the Council's security policies and/or procedures to the police for investigation and (if appropriate) the institution of criminal proceedings if in the reasonable opinion of the Council such breach has or is likely to lead to the commissioning of a criminal offence.

4.5 If you do not understand the implications of this policy, any of the policies referred to within it or how the policies may apply to you, please seek advice from your line manager, ICT or Information Security Manager.

4.6 In the event of an apparent breach of the policies, by a user, a group of users, the ICT department has authority to withdraw access temporarily or permanently to all or any subset of ICT facilities, including but not limited to;
Network (Active Directory)
Emails and Internet
ICT Business Systems
Remote Access Systems

4.7 In the event of an apparent breach of the policies, by a user, a group of users, the ICT department has authority to seize and quarantine any ICT equipment and peripherals as part of any investigation into user(s) activities.

5 Risks

Dacorum Borough Council recognises that there are risks associated with users accessing and handling information in order to conduct official Council business.

This policy aims to mitigate the following risks:

- Non-compliance with Data Handling Guidelines and the GDPR / Data Protection Act 2018
- loss of personal information
- loss of information
- Identity theft
- Increased points of access for information (risks around multiple agency sharing)
- Information Security Breaches
- Ineffective or inappropriate access to systems and data
- Fines associated with information access or security breaches

Non-compliance with this policy could have a significant effect on the efficient operation of the Council and may result in financial loss and an inability to provide necessary services to our customers**.**

6 PSN / (GCSx) Acceptable Usage Policy

Each PSN / (GCSx) user must read, understand and sign to verify they have read and accepted this policy.

- I understand and agree to comply with the security rules of my organisation.

For the avoidance of doubt, the security rules relating to secure e-mail and information systems usage include:

1. I acknowledge that my use of the PSN / (GCSx) may be monitored and/or recorded for lawful purposes.

2. I agree to sign the associated policies

3. I agree to use a 'managed device' owned by the Council, and will use that device to access PSN / GCSx information in accordance with the Council's security procedures.

4. I agree to be responsible for any use by me of the PSN / (GCSx) using my unique user credentials (user ID and password, access token, direct access or other mechanism as provided) and e-mail address; and,

5. will not use a colleague's credentials to access the PSN / (GCSx) and will equally ensure that my credentials are not shared and are protected against misuse; and,

6. will protect such credentials at least to the same level of secrecy as the information they may be used to access, (in particular, I will not write down or share my password other than for the purposes of placing a secured copy in a secure location at my employer's premises); and,

7. will not attempt to access any computer system that I have not been given explicit permission to access; and,

8. will not attempt to access the PSN / (GCSx) other than from ICT equipment and systems and locations which have been explicitly authorised to use for this purpose; and,

9. I will not access PSN/GCSx material via an unmanaged device or insecure method (e.g. Outlook Web Access)

10. I agree that if I will only use my dacorum.gov.uk email account to transmit / receive OFFICIAL, OFFICIAL-SENSITIVE information.

11. will not transmit information via the PSN / (GCSx) that I know, suspect or have been advised is of a higher level of sensitivity than my PSN / (GCSx) domain is designed to carry; and,

12. will not transmit information via the PSN / (GCSx) that I know or suspect to be unacceptable within the context and purpose for which it is being communicated; and,

13. will not make false claims or denials relating to my use of the PSN / (GCSx) (e.g. falsely denying that an e-mail had been sent or received); and,

14. will protect any sensitive or not protectively marked material sent, received, stored or processed by me via the PSN / (GCSx) to the same level as I would paper copies of similar material; and,

15. will appropriately label, using the GPMS, information up to Restricted sent via the PSN / (GCSx); and,

16. will not send Protected or Restricted information over public networks such as the Internet; and,

17. will always check that the recipients of e-mail messages are correct so that potentially sensitive or Protected or Restricted information is not accidentally released into the public domain; and,

18. will not auto-forward email from my .gov.uk account to any other non-GCSx email account; and,

19. will not forward or disclose any sensitive or Protected or Restricted material received via the PSN / (GCSx) unless the recipient(s) can be trusted to handle the material securely according to its sensitivity and forwarding is via a suitably secure communication channel; and,

20. will seek to prevent inadvertent disclosure of sensitive or Protected or Restricted information by avoiding being overlooked when working, by taking care when printing information received via PSN / (GCSx) (e.g. by using printers in secure locations or collecting printouts immediately they are printed, checking that there is no interleaving of printouts, etc) and by carefully checking the distribution list for any material to be transmitted; and,

21. will securely store or destroy any printed material; and,

22. will not leave my computer unattended in such a state as to risk unauthorised disclosure of information sent or received via PSN / (GCSx) (this will be in accordance with DBC001 IS Policy – Corporate Information Security Policy and DBC010 Corporate Information Technology Security Policy - e.g. logging-off from the computer, activate a password-protected screensaver etc, so as to require a user logon for activation); and,

23. where ICT Services has implemented other measures to protect unauthorised viewing of information displayed on ICT systems (such as an inactivity timeout that causes the screen to be blanked requiring a user logon for reactivation), then I will not attempt to disable such protection; and,

24. will make myself familiar with the Council's security policies, procedures and any special instructions that relate to PSN / (GCSx); and,

25. will inform my manager immediately if I detect, suspect or witness an incident that may be a breach of security; and,

26. will not attempt to bypass or subvert system security controls or to use them for any purpose other than that intended; and,

27. will not remove equipment or information from council premises without appropriate approval; and,

28. will take precautions to protect all computer media and portable computers when carrying them outside my organisation's premises (e.g. leaving a laptop unattended or on display in a car such that it would encourage an opportunist theft) in accordance with the Council's DBC700 IS - Remote and Home Working Policy; and,

29. will not introduce viruses, Trojan horses or other malware into the system or PSN / (GCSx); and,

30. will not disable anti-virus protection provided at my computer; and,

31. will comply with the General Data Protection Regulations (GDPR) Data Protection Act 2018 and any other legal, statutory or contractual obligations that the Council informs me are relevant (please refer to the Data Protection Policy - DBC100 IM GDPR / UK Data Protection Act Policy

32. if I am about to leave the Council, I will inform my manager prior to departure of any important information held in my account and manage my account in accordance with the Council's email and records management policy.

Document Date:	[Date signed and agreed by staff member]
Name of User:	[Surname, First Name]
Position:	[Position]
Department:	[Department]
User Access Request Approved by:	[Line Manager Name – Position} [Date]
User Access Request Approved by:	[ICT Services Asset Owner(s)] [Date]
User Access Request Processed:	[ICT Services] [Date]

7 PSN / (GCSx) Personal Commitment Statement

I, [insert User's Name], accept that I have been granted the access rights to PSN / (GCSx). I understand and accept the rights which have been granted, I understand the business reasons for these access rights, and I understand that breach of them, and specifically any attempt to access

services or assets that I am not authorised to access, may lead to disciplinary action and specific sanctions. I also accept and will abide by this Acceptable Usage Policy.

I understand that failure to comply with this agreement, or the commission of any information security breaches, may lead to the invocation of the Council's disciplinary policy.

Signature of User: ……

A copy of this agreement is to be retained by the User and Line Manager.

8 Policy Governance

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

- **Responsible** – the person(s) responsible for developing and implementing the policy.
- **Accountable** – the person who has ultimate accountability and authority for 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.

Responsible	Information Security Manager
Accountable	Assistant Director – Legal Governance
Consulted	CMT, AD's / GM's
Informed	All

9 Review and Revision

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

Policy review will be undertaken by the Information Security Manager

10 References

The following Dacorum Borough Council policy documents are directly relevant to this policy, and are referenced within this document

DBC001 IS Corporate Information Security Management Policy
DBC010 IS Corporate Information Technology Security Policy
DBC100 IM GDPR / UK Data Protection Act Policy
DBC700 IS Remote and Home Working Policy
DBC900 IS Information Security Incident Reporting Policy

DBC999 IS Proc – Personal Data Breach or Incident Reporting Procedure.
Remote and Home Working Guidance

11. Glossary

Managed Device - device owned by the Council, i.e. Laptop. Device must be encrypted, patched and running anti-virus. Device must be used in conjunction with two-factor authentication.

PSN - Public Services Network, access to IL2 / IL3 data. GCsx / GSi will be subsumed into PSN

Two Factor – a means of authenticating access credentials, by way of a password and secure token to generate a random PIN

Document Control

Author:	John Worts - Information Security Manager
Owner:	Mark Brookes, Assistant Director – Corporate and Contracted Services
Document Version	1.5
Full Document Title	DBC170 IS Policy – Government Connect (PSN / (GCSx) Acceptable Usage Policy

Revision History

Revision Date	Previous Revision Date	Previous Revision Level	Summary of Changes	Changes Marked	Next Review Date
2009	n/a	n/a	First Draft		
23/12/09	2009	0.1	Includes Restricted Data Definitions		
16/5/12	23/12/09	0.2	Revised title to conform to new IS and IM Policy Structures		
11/7/12	16/5/12	1.0	References to IA Document Structure		July 2013
7/10/13	11/7/12	1.1	Added PSN to cover scope of new services. Added Glossary and amended policy to reflect use of managed devices		October 2014
29/03/16	7/10/13	1.2	Title Change and added DBS / DS		
25/5/18	1/5/18	1.3	GDPR / Data Protection Act 2018		May 2019

5/8/19	25/5/18	1.4	GCSx Email accounts reference removed as dacorum.gov.uk approved for transmission of OFFICIAL material		August 2020

11 Appendix 1 – Impact Level Assessments

Business Impact Level 0 (BIL0) - NO IMPACT

- Not likely to cause any specific loss but may cause some embarrassment if information were to fall into the wrong hands

Business Impact Level 1 (BIL1) - UNCLASSIFIED or NON PROTECTIVELY MARKED assets

- To cause a Financial Loss to the Public Sector of up to £1,000.00
- Likely to cause a Minor Financial Loss to any party - for example under £100.00 for an Individual or Sole Trader or up to £1,000.00 for a Larger Business

Business Impact Level 2 (BIL2) - Criteria for assessing PROTECT assets:

- Likely to cause distress to individuals
- Breach proper undertakings to maintain the confidence of information provided by third parties
- Breach statutory restrictions on the disclosure of information
- Cause financial loss or loss of earning potential, or to facilitate improper gain
- Unfair advantage for individuals or companies
- Prejudice the investigation or facilitate the commission of crime
- Disadvantage government in commercial or policy negotiations with others
- Likely to cause inconvenience or loss to an individual or
- Would undermine the Financial Viability to UK SME's (Small and Medium sized Enterprises)
- Can potentially cause a Financial Loss to the Public Sector of up to £10,000.00
- Likely to cause a Moderate Financial Loss to any party - for example under £1,000.00 for an Individual or Sole Trader or under £10,000.00 for a Larger Business

Business Impact Level 3 (BIL3) - Criteria for assessing RESTRICTED assets:

- Affect Diplomatic relations adversely
- Cause substantial distress to individuals
- Make it more difficult to maintain the operational effectiveness or security of United Kingdom or Allied forces
- Cause financial loss or loss of earning potential or to facilitate improper gain or advantage for individuals or Companies
- Prejudice the investigation or facilitate the commission of crime
- Breach proper undertaking to maintain confidence of information provided by 3rd parties
- Impede the effective development or operation of government policies
- To breach statutory restrictions on disclosure of information
- Disadvantage government in commercial or policy negotiations with others
- Undermine the proper management of the public sector and its operations
- Likely to cause a risk to an Individuals Safety and Liberty
- Would undermine the Financial Viability of a Minor UK based or UK owned Organisation
- Can potentially cause a financial loss to HMG/Public Sector of up to £1million
- Likely to cause a Significant Financial Loss to any party - for example under £10,000.00 for an Individual or Sole Trader or under £100,000.00 for a Larger Business