PSN (Public Services Network) Acceptable Usage Policy

Policy Statement

It is the Council's policy that all users of the PSN understand and comply with corporate commitments and information security measures associated with the PSN.

Purpose

PSN stands for Public Services Network. It is a secure private Wide-Area Network (WAN) which enables secure interactions between connected public sector organisations e.g. Local Authorities, DWP etc

Some Council employees 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 employees having access to a secure email facility (also know as GCSx email). All employees requiring access to the PSN in any way will be required to read and understand this Acceptable Usage Policy (AUP) and sign the Personal Commitment Statement. This policy and statement does not replace the Council's existing acceptable usage, or any other, policies. It is a supplement to them.

Scope

This policy applies to ALL users of the PSN connection including email, and system access. All users must be aware of their commitments and the security measures surrounding the use of this network.

This policy must be adhered to at all times when accessing PSN facilities.

Baseline Personnel Security Standard (BPSS)

It is a requirement of the PSN Code of Connection that all staff with access to the PSN Secure email or PSN Secure information systems have undertaken a full BPSS (Baseline Personnel Security Standard) or equivalent checks.

The BPSS is the minimum standard required to ensure the identity and integrity of an employee with access to sensitive information. It involves four main elements:

- An appropriate identity check
- Confirmation of Nationality & Immigration Status
- Employment history (for the past 3 years)
- Third-party verification of unspent convictions

Third-party verification of unspent convictions requires external checks to be undertaken and must be completed and verified by HR before this application is submitted to ICT for access to PSN facilities. There may be a cost for this service, which is not funded by ICT services. The Line manager will authorise the Access request form by signing the form, which will confirm that BPSS checks have been undertaken and verified by HR.

PSN Facilities

PSN Secure Email (also known as GCSx email) – For the secure transmission of emails to other PSN/GCSx email accounts. Emails sent from PSN/GCSx mailboxes can ONLY be sent to secure email domains connected to the PSN (the most common ones are .gcsx.gov.uk .gsi.gov.uk, .gsx.gov.uk, pnn.gov.uk, gse.gov.uk – *contact ICT for a complete up to date list*) - this is to prevent secure mail being inadvertently sent to an insecure address. Emails originating from PSN/GCSx mailboxes should conform to the GSC (Government Security Classification) standards which is a mandatory requirement for labelling PSN/GCSx emails. The GSC replaced the Government Protective Marking System (GPMS) in April 2014.

Secure Information Systems – For access to secure PSN systems including

- DWP Customer Information System (CIS)
- DTA (Data Transfer Appliance for Revs and Bens)
- Tell Us Once
- CESG IA Portfolio
- LoCTA Service
- Individual Electoral Registration
- Government Gateway EAS Service
- ePIMS (Electronic Property Information Management System)

PSN Acceptable Usage Policy

Each PSN 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.

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

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

- I will not use a colleague's credentials to access the PSN and will equally ensure that my credentials are not shared and are protected against misuse;
- I will not attempt to access any computer system that I have not been given explicit permission to access;
- I will not attempt to access the PSN other than from ICT equipment provided by the Authority (this excludes ALL personal IT equipment for PSN use),
- I will not transmit information via the PSN that I know or suspect to be unacceptable within the context and purpose for which it is being communicated;
- I will not make false claims or denials relating to my use of the PSN (e.g. falsely denying that an e-mail had been sent or received);
- I will 'mark' any email created with the appropriate Government Security Classification (GSC) label (See Appendix A)
- I will protect any material, whatever the sensitivity or protective marking, sent, received, stored or processed by me via the PSN to the same level as I would paper copies of similar material;
- I will not send sensitive or protectively marked information received, stored or processed by me via the PSN to a non PSN e-mail account i.e. over the internet or to a .gov.uk account.
- I will always check that the recipients of e-mail messages are correct so that potentially sensitive or protectively marked information is not accidentally released into the public domain;
- I will not auto-forward e-mail from my PSN e-mail account to any other non-PSN e-mail account;
- I will not use any PSN email address as a sender field when emailing content from the internet;
- I will not forward or disclose any sensitive or protectively marked material received via the PSN 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;

- I will seek to prevent inadvertent disclosure of sensitive or protectively marked information by avoiding being overlooked when working, by taking care when printing information received via PSN (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;

- I will securely store or destroy any printed material;

- I will not leave my computer unattended in such a state as to risk unauthorised disclosure of information sent or received via the PSN e.g. By closing the e-mail program, logging-off from the computer, activating a password-protected screensaver, etc., so as to require a user logon for activation;

- Where my organisation has implemented other measures to protect ICT systems, then I will not attempt to disable or bypass such protection;

- will adhere to the Council's IT Security policies;

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

- I will not remove equipment or information from my organisation's premises without appropriate approval;

- 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);

- I will not knowingly introduce viruses, Trojans or other malware into the system or the PSN;

- I will not disable anti-virus protection provided at my computer;

- I will comply with the Data Protection Act 1998 and any other legal, statutory or contractual obligations that the Council informs me are relevant;

- If I am about to leave my employer, I will inform my manager prior to departure of any important information held in my account.

Policy Compliance

If any user is found to have breached this policy, they may be subject to the Authority's disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

If you do not understand the implications of this policy or how it may apply to you, seek advice from ICT Services.

Policy Governance

The following identifies who within the Authority is Accountable, Responsible, Informed with regards to this policy. The following definitions apply:

	Definition	Role
Responsible	the person(s) responsible for developing and implementing the policy.	Head of ICT Services or equivalent
Accountable	the person who has ultimate accountability and authority for the policy.	Section 151 Officer
Informed	the person(s) or groups to be informed after policy implementation or amendment.	PSN/GCSx email Users

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 ICT Manager.

References

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

•• SS_POL018_Information Security Policy

Appendix A – Protective Marking Guidelines

Protective Marking

Protective marking is the practice of adding a security label to data and/or documents so that everyone who comes into contact with it understands who it could be released to.

The Government Security Classifications Policy (GSCP) simplified and replaced the Government Protective Marking System (GPMS) in April 2014. The GSCP details three security classifications (of which only the lowest is used by local authorities), namely:

• OFFICIAL - The majority of information that is created or processed by the public sector. This includes routine business operations and services, some of which could have damaging consequences if lost, stolen or published in the media, but are not subject to a heightened threat profile

• SECRET - Very sensitive information that justifies heightened protective measures to defend against determined and highly capable threat actors. For example, where compromise could seriously damage military capabilities, international relations or the investigation of serious organised crime.

• TOP SECRET – HMG's most sensitive information requiring the highest levels of protection from the most serious threats. For example, where compromise could cause widespread loss of life or else threaten the security or economic wellbeing of the country or friendly nations.

The definition of OFFICIAL is defined as:

Definition:

ALL routine public sector business, operations and services should be treated as OFFICIAL

- many departments and agencies will operate exclusively at this level.

This includes a wide range of information, of differing value and sensitivity, which needs to be defended against the threat profile described in paragraph 15 above, and to comply with legal, regulatory and international obligations.

This includes:

- The day to day business of government, service delivery and public finances.
- Routine international relations and diplomatic activities.
- Public safety, criminal justice and enforcement activities.
- Many aspects of defence, security and resilience.
- Commercial interests, including information provided in confidence and intellectual property.
- Personal information that is required to be protected under the Data Protection Act (1998) or other legislation (e.g. health records).

Baseline Security Outcomes:

- ALL Council & HMG information must be handled with care to prevent loss or inappropriate access, and deter deliberate compromise or opportunist attack.
- Staff must be trained to understand that they are personally responsible for securely handling any information that is entrusted to them in line with local business processes.
- Baseline security controls reflect commercial good practice

Marking:

There is no requirement to explicitly mark routine OFFICIAL information. Baseline security measures should be enforced through local business processes.

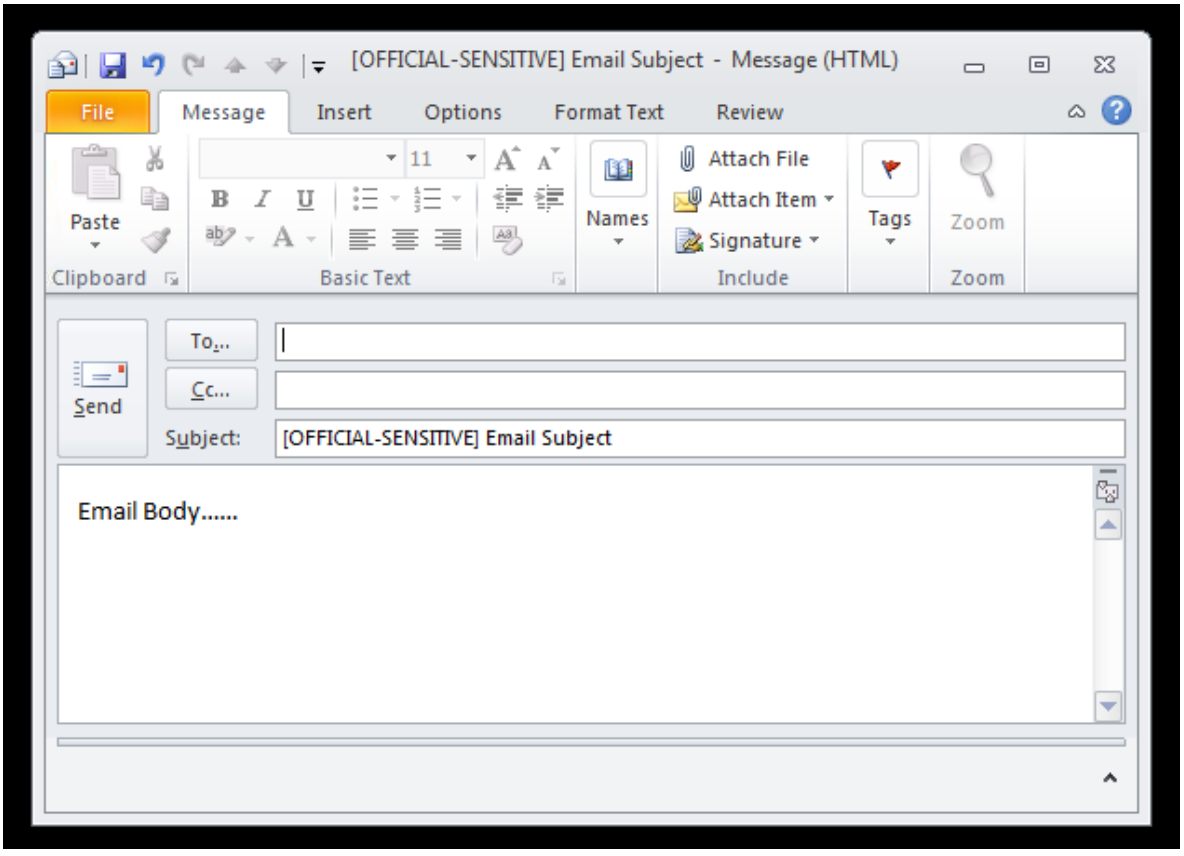
A limited subset of OFFICIAL information could have more damaging consequences (for individuals, an organisation or government generally) if it were lost, stolen or published in the media. This subset of information should still be managed within the 'OFFICIAL' classification tier, but may attract additional measures (generally procedural or personnel) to reinforce the "need to know". In such cases where there is a clear and justifiable requirement to reinforce the "need to know", assets should be conspicuously marked: "OFFICIAL–SENSITIVE"

Responsibilities
New Emails that contain sensitive data must be marked in the header subject with “[OFFICIAL-SENSITIVE]”. Data can be marked as “[OFFICIAL]” but it is not a requirement.

Information received from an external source must be marked by the recipient, who becomes its owner. E.g. you receive an email with an attachment, and you must decide on its security label before saving or sharing either the email or attachment.

Information received from an Internal source must be marked by the owner, who is responsible for its security label.

Example Marking of Email Subject Headers
Emails should be marked as follows



This page is intentionally blank – please do not delete as it allows the following form to be removed from the document.

Blaby District Council
the heart of Leicestershire

Hinckley & Bosworth Borough Council
A Borough to be proud of

Melton Borough Council

Oadby and Wigston Borough Council

PSN Access Request Form

To be completed by the Line Manager

Name of User requiring access		**Job Title/ Position:**	
Name of Employing organisation			
Service Area:			

Type of Access Required	PSN (GCSx) Secure Email ☐ Yes ☐ No	Secure System Access ☐ Yes ☐ No

Name of Line Manager		**Job Title/ Position:**	
Signature of Line Manager *(Authorising use of PSN & BPSS check confirmed)*	***Full BPSS (or equivalent) checks must be confirmed by HR prior to Signing***		
Date			

To be completed by the User

PSN Personal Commitment Statement

I, ……..accept that I have been granted the access rights to PSN. 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 policy, personal commitment statement, and other Council policies under the terms of my contract of employment. 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 ICT.