IT Services

All staff must agree to the following personal commitment in order to use the Council's systems. It contains elements from the full Information Security Policy, which should be referred to for detailed guidance. This is intended to help protect both the Council and yourself from the risks of a data security incident.

I understand and agree to comply with the Information Security Policy, security procedures and other relevant policies and procedures of Gedling Borough Council all of which are published on the Intranet;

I acknowledge that my use of the computer systems may be monitored and/or recorded;

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

I will protect any sensitive or protectively marked information sent, received, stored or processed by me to the same level as I would paper copies of similar material;

I will ensure all equipment and software is used correctly by following any User Guides, instructions, manuals or training which is available;

I will ensure that Council data is protected by making sure there is an up to date copy on a network location which is backed up;

I will always check that the recipients of e-mail messages and faxes are correct so that potentially sensitive or protectively marked information is not accidentally released into the public domain;

I will seek to prevent inadvertent disclosure of sensitive or protectively marked information by avoiding being overlooked when working, by taking care when printing by using printers in secure locations or collecting printouts immediately they are printed, checking that there is no interleaving of printouts and by carefully checking the distribution list for any material to be transmitted;

I will securely store or destroy any printed material;

I will seek clarification, if unsure, of any policy, procedure or rule from my manager or the ICT department;

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

I will be mindful that people may attempt to bypass the Council's security, obtain passwords, or access information by deception, known as social engineering;

I will inform my manager if I become aware of any weaknesses in any existing procedure, computer system, policy or working practice that could in the future lead to loss of sensitive information or disruption to services;

I will take precautions to protect all computer media and portable computers when carrying them outside my organisations premises (e.g. not leaving a laptop unattended or on display in a car such that it would encourage an opportunist thief);

I will make myself familiar with the Information Security Policy, security procedures and any special arrangements in my area;

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

If I am about to leave the Council's employ, I will inform my manager prior to departure of any important information held in my account and return all equipment;

I will not use a colleague's credentials and will equally ensure that my credentials are not shared and are protected against misuse;

I will not send sensitive or protectively marked information over public networks such as the Internet or email unless properly encrypted;

I will not forward or disclose any sensitive or protectively marked material 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 not leave my computer unattended in such a state as to risk unauthorised disclosure of information by logging off, or locking the screen for short periods;

I will not attempt to access any computer system that I have not been given explicit permission to access and will only use such systems for authorised purposes;

I will not attempt to bypass or subvert system security controls, including anti-virus, and will ensure any laptop or similar network connected device has up to date security controls by connecting it to the network once a week;

I will not remove equipment or information from the Council's premises without appropriate approval;

I will not transfer sensitive or protectively marked information off site without authorisation, or use unencrypted devices to carry this data;

I will not connect personal, unauthorised or 3rd Party devices to the computers or networks;

I will not knowingly introduce viruses, Trojan horses or other malware to the Council's computers or networks;

I will not download or install software on any PC or device, or run unauthorised programs;

I will not use any system to view or transmit inappropriate material which may damage the reputation of the Council or is unlawfully in any way;

I will not use any system to harass, libel or slander another person, nor produce, obtain, store, display or distribute material that is likely to cause offense;

I understand that failure to adhere to the Information Security Policy may be treated as a matter of misconduct, or potentially gross misconduct as defined within the Council's Disciplinary Procedure which may if proven, and after proper application of this procedure, lead to termination of employment.

Signature	
Print Name	
Date	