

## 3. Device Configuration

Device configuration consists of Configuration Words, Code Protection, Device ID and Rev ID.

### 3.1 Configuration Words

There are six Configuration Word bits that allow the user to setup the device with several choices of oscillators, Resets and memory protection options. These are implemented as Configuration Word 1 through Configuration Word 6 at 300000h through 30000Bh.



**Important:** The  $\overline{\text{DEBUG}}$  bit in Configuration Words is managed automatically by device development tools including debuggers and programmers. For normal device operation, this bit should be maintained as a '1'.

### 3.2 Code Protection

Code protection allows the device to be protected from unauthorized access. Program memory protection and data memory are controlled independently. Internal access to the program memory is unaffected by any code protection setting.

#### 3.2.1 Program Memory Protection

The entire program memory space is protected from external reads and writes by the  $\overline{\text{CP}}$  bit. When  $\overline{\text{CP}} = 0$ , external reads and writes of program memory are inhibited and a read will return all '0's. The CPU can continue to read program memory, regardless of the protection bit settings. Self-writing the program memory is dependent upon the write protection setting.

#### 3.2.2 Data memory protection

The entire Data EEPROM Memory space is protected from external reads and writes by the  $\overline{\text{CPD}}$  bit. When  $\overline{\text{CPD}} = 0$ , external reads and writes of Data EEPROM Memory are inhibited and a read will return all '0's. The CPU can continue to read Data EEPROM Memory regardless of the protection bit settings.

### 3.3 Write Protection

Write protection allows the device to be protected from unintended self-writes. Applications, such as boot loader software, can be protected while allowing other regions of the program memory to be modified.

The [WRT](#) bits define the size of the program memory block that is protected.

### 3.4 User ID

Eight words in the memory space (200000h-200000Fh) are designated as ID locations where the user can store checksum or other code identification numbers. These locations are readable and writable during normal execution. See the "User ID, Device ID and Configuration Word Access" section for more information on accessing these memory locations. For more information on checksum calculation, see the "PIC18(L)F27/47K40 Memory Programming Specification", (DS40001772).

#### Related Links

[User ID, Device ID and Configuration Word Access](#)