CHAPTER 42 – INFORMATION SYSTEMS

Included in this Chapter:

PART A: EMAIL, COMPUTERS, ETC.

42.01 Purpose

Electronic mail, Internet and telecommunications access are resources made available to city employees to communicate with each other, other governmental entities, companies and individuals for the benefit of the City. The City has established a policy regarding access and disclosure of electronic mail messages created, sent or received by City employees. This policy applies to external (Internet) electronic mail, as well as the City's internal electronic mail system.

42.02 Policy

The City of Middletown provides e-mail to its employees to assist and facilitate business communications. It is provided for legitimate business use in the course of an employee's assigned duties only. Inappropriate use may result in the loss of access privileges and disciplinary action up to and including dismissal.

The City reserves the right to access and disclose all messages created, received, or sent over its electronic mail system for any purpose. The City reserves the right to disclose any e-mail message to City or law enforcement officials without the permission of the employee.

The use of passwords for security does not guarantee privacy or confidentiality. The use of a password or code does not restrict the City's right to access electronic communications. Upon request, all passwords must be disclosed to the City.

All data and other electronic messages within this system are the property of the City. E-mail messages may qualify as public records and may be subject to the Public Records Act, depending on the content. E-mail is not the private property of any employee.

In addition, the City, through its managers and supervisors, reserves the right to review the contents of employee's e-mail communications when necessary for City business purposes. Employees may not intentionally intercept, eavesdrop, record, read, alter or receive other person's e-mail messages without proper authorization.

The City of Middletown, through its Information Systems Division, purchases, owns and administers the necessary software and licenses to provide access to e-mail and Internet services. Employees may not rent, copy or loan the software, or its documentation. The City has invested much time and money to secure its electronic systems from intrusion and harmful malware. Therefore, employees may not provide alternative software to access the system. Employees may be held responsible for any damages caused by unauthorized software or malware they introduce into the system. Department Directors are responsible for the implementation and adherence of this policy within their departments.

42.03 Prohibited Uses

When sending e-mail messages, good judgment should be used. The following are examples of conduct that is prohibited:

- Unauthorized attempts to access another's e-mail messages;
- Transmission of sensitive, confidential, proprietary, copyrighted, or other similar information to unauthorized persons or organizations;
- Transmission of inappropriate, obscene, offensive, harassing, or disruptive messages;
- Any illegal or unethical activity which could adversely affect the City;
- Any non-job related solicitation;
- Any message sent to all users of the City e-mail system that does not have the prior approval of the City Manager's office;
- Communications of sexually explicit images or messages;
- Communications that contain ethnic slurs, racial slurs, or anything that may be construed as harassment or disparagement off others based on race, national origin, sex, age, disability or religious belief; or
- Any other use that may compromise the integrity of the City and/or its business in any way.

42.04 Retention of E-Mail

E-mail shall not be used for document retention or archival purposes. E-mail shall be retained for a period not to exceed thirty days, and shall then be destroyed. Each employee is responsible for the review and purging of his/her own e-mail. If it is necessary to retain e-mail, hard copies should be printed.

No employee shall, without the prior express permission of the Information Systems Manager, download any file or attachment to an e-mail message from the Internet or from any non-City computer system.

Generally, e-mail messages are intended to be temporary communications that are non-vital and may be discarded routinely. However, depending on the content of the e-mail message, it may be considered a more formal record and should be retained pursuant to a department's record retention schedules. As such, these e-mail messages are similar to printed communication and should be written with the same care. Each department head is responsible for establishing and maintaining department retention schedules for the information communicated through the e-mail system.

However, employees should be aware that when they have deleted a message from their workstation mailbox, it might not have been deleted from the central e-mail system. The message may be stored on the computer's back-up system for an indefinite period. Written communications to and from public officials or public employees, including e-mails, are subject to the Ohio Public Records Act, and in most cases must be made available to any person, including the media, upon request. E-mail, which qualifies as a public record, will be released, unless it clearly falls under a specific exemption in the state law.

42.05 Basic Computer Security

A. Passwords & Passphrases

Each computer user is responsible for choosing a strong password that is known only to that user. Upon request, all passwords must be disclosed to the City. As a general rule, longer passwords are stronger than shorter passwords. The combination of multiple, unrelated words can form the basis for a strong password, often termed a "passphrase". A passphrase can be more easily

remembered, and is stronger than a shorter, more complex password.

Make sure that the words you use are truly random and not just common phrases, quotes, song lyrics, book titles, etc. Contemporary password cracking tools will not have any trouble with a passphrase of that nature.

A good target to shoot for is a passphrase that contains at least three or four truly unrelated words, and that is at least twelve (12) characters long. Some systems may not allow that many characters in a password, but it is a good starting point.

When you select a passphrase, you can make it even stronger by adding numbers or special characters that will change the words in the passphrase to non-dictionary words. You should incorporate a minimum of one uppercase, one numeric, and one special character.

Passwords must be memorized by the user, and must not be written down or posted in any location that the password would be discovered by an unauthorized person. Passwords must be kept secret; If an employee suspects that his/her password has been become known to someone else, or has in some other way been compromised, the employee must immediately notify the Information Systems Manager.

Passwords will be changed frequently. An employee may change their password as often as they wish. The City's computer system will force a password change on a regular basis.

If an employee is using a mobile phone or device to access City email, Information Systems must be notified immediately if the device is lost, and the employee must change their password.

Users of mobile computing devices will likely be required to use a smart card or other two-factor authentication.

B. Workstation Security

Employees should log off their computers whenever they leave their workstation, even if the trip is expected to be brief. It is a serious breach of security to walk away from a computer that the employee is logged into. Logging off at the end of the work day is mandatory.

C. Backups of Workstation Data

All important data files (Word documents, Excel spreadsheets, etc.) must be stored on the virtual drives, H:, I:, K:, so that they can be backed up when the City's servers are backed up. Only temporary and interim files should be stored on the C: drive of the employee's local workstation.

42.06 Workstation Software Licenses

Each department is responsible for purchasing a licensed copy of every application software package running on each individual workstation. Software licensing policies must be strictly adhered to. It is illegal and unethical to "bootleg" software, or to make unauthorized copies that are outside the scope of the software manufacturer's licensing policies.

Each department is responsible for reading and enforcing the software licensing requirements for applications running on every workstation within the department. Each department is responsible for maintaining the manufacturer's proof of ownership for every piece of application software residing on individual workstations within the department.

Information Systems will conduct regular audits to check conformance to software licensing policies.

42.07 Authorized Workstation Software

Only software that permits an employee to accomplish the duties outlined in the employee's Job Description should be installed on the employee's workstation. No auxiliary software shall be installed on individual workstations without the prior approval of the Information Systems Manager.

42.08 Application Software Usage

A. No employee shall access or attempt to access applications for which he/she does not have authorized security clearance. Department Managers shall submit a signed, written "Security Clearance" form listing the applications each employee should be allowed to access. Information Systems will review the requested applications, set up appropriate system access, sign-off on the Security Clearance form and maintain a current file of approved Security Clearance forms.

B. Electronic Bulletin Board System (BBS). All requests for messages to be posted to the City BBS must be submitted to the City Manager's office. Only the City Manager's office and Information Systems shall be permitted to add, modify, and delete messages on the City BBS. Only work-related messages or other appropriate messages will be approved.

42.09 Usage of Central Computer Virtual Drives

Disk space is maintained on the City's central computers so that inter-departmental and intra-departmental document and data file sharing may be accomplished. The following is a list of the virtual drives on the central computers and their intended usage:

Drive	Description	Purpose
G:	City drive	Temporary City-wide file sharing
H:	Departmental drive	Inter-departmental file sharing
I:	Individual drive	Individual user file storage and work area
K:	Agendas drive	Work area for City Council agendas

The G: drive is provided for temporary and interim storage of files. None of the files on the G: drive should be considered confidential or private since every City computer user has access to this drive. Any data file on the G: drive is subject to removal without notice after 60 days.

The H:, I:, and K: drives are provided for more secure, longer-term storage of files, with the provision of the files being backed

up every night. Access to these drives is more restricted, but any confidential or sensitive documents should be protected with a password.

Each City computer user is assigned an I: drive that is only accessible by that individual. An employee's data files and documents should be stored on their I: drive rather than on the C: drive of their workstation. The I: drives are automatically backed up every night. Workstation C: drives DO NOT get backed up.

The J: and O: drives are dedicated to special uses and should only be utilized with the permission and assistance of the Information Systems Division.

Programs should never be installed on a virtual drive or on any City server without the prior approval of the Information Systems Division.

42.10 Internet Usage

Goals and objectives for use of the Internet include the facilitation of communications, information access, and information sharing for City employees. The Internet has the potential to enhance an employee's access to and use of relevant job-related information and knowledge. Effective use of the Internet should result in a more informed, knowledgeable, and productive employee. The City maintains access to the Internet to assist all employees in conducting business. The City encourages furthering employee's knowledge through appropriate use of Internet resources. This policy applies to all employees who have access to the Internet.

As with printed information, not all sources on the Internet provide accurate, complete or current information. Users should evaluate Internet sources just as they would printed publications, and question the validity of the information provided.

A. Use

1. Authorized use of the Internet is outlined as follows:

- Use related to non-confidential or non-proprietary City business.

- Use in accordance with City requirements pertaining to records management (retention and disposal), security (classification of information) and copyrights.
- Use according to any associated terms and conditions specified by the supplier of the information to be downloaded.
- Use in accordance with all applicable laws, regulations, policies and procedures. The Internet is an international service. State, national and international laws may be applicable.

2. Unauthorized use of the Internet is outlined as follows:

   - Unauthorized sending, receiving or downloading of copyrighted materials, confidential information including trade secrets, proprietary financial information, or similar materials.
   - Private commercial ventures, religious or political causes for personal gain or public persuasion.
   - Illegal activities or those which would adversely affect the interest of the City.
   - Offensive or disruptive materials. Those materials considered offensive include any sexually explicit materials, racial slurs, or materials that offensively address someone's age, sexual orientation, religious or political beliefs, nationality or disability.
   - Downloading or executing files that may infect City computer systems with malware.
   - Expression of personal views or opinions that could be misinterpreted as those of the organization.

3. Any employee who disregards the City Internet policy, and is found to be in violation, shall be subject to disciplinary action, up to and including termination.

B. Data Protection

Users of the Internet should not assume that they are provided any degree of protection for data transmitted over the network. Users are advised not to submit personal

details or confidential information that could potentially be misused.

C. Ownership

The hardware, software and computer network are considered to be City property. All information sent or received through the Internet is and will remain the property of the City. This information is not the private property of any employee.

The City reserves and intends to exercise the right to review, audit, intercept, access and disclose any information created, received, downloaded or sent through the Internet or City computer network for any purpose. If an employee is suspected of misusing access to the Internet, his or her supervisor will be notified so that further monitoring and/or corrective action may take place.

D. Security

Users of Internet services should be aware of their responsibility to protect City network security. The City's Internet firewall is intended to protect the internal computer network from unauthorized access from the public Internet. The Internet lacks the controls and management normally applied to the City's computer network to protect information privacy. No protection is provided once the user is out on the public Internet.

Encryption is the only means available to ensure privacy of any information on the Internet. Currently the only means of encryption available require individuals to perform the encryption function themselves before sending information to the Internet. Anything not encrypted should be regarded as available for viewing not only by the intended recipient, but also any other unknown person.

Downloading from the Internet should only be done with the assistance of Information Systems, after receiving the permission of the Information Systems Manager. All executable files should be virus checked and initially run in a test environment to ensure the integrity of the information received. Malware is present in webpages, applications, e-mail attachments, word processing documents, spreadsheets and any other file type. The only protections

against downloading malware are restricting downloading and scanning all files before they are used.

Users shall ensure that software acquisition and utilization adheres to applicable software licenses and copyright law. Users shall maintain documentation sufficient to prove that all software installed on any computer workstation assigned to them has been legally obtained and is installed in conformance with applicable license(s).
ONLY SOFTWARE THAT HAS BEEN APPROVED BY THE INFORMATION SYSTEMS MANAGER SHALL RESIDE ON CITY COMPUTERS.

E. Authority

Access to the Internet will be provided by Information Systems only through a written request from an employee's Department Director

Department Directors and Division Managers will have authority to monitor an employee's activities on the Internet.

Information Systems must approve all software/hardware acquisitions to ensure compatibility with City systems. This includes the receipt/or ordering of hardware/software via E-mail or the Internet.

F. Discipline

1. Any employee who disregards the City Internet Policy, and is found to be in violation, shall be subject to disciplinary action, up to and including termination.

2. The City will require employees to read and signify acceptance of the terms of this policy by signing the following agreement before making electronic systems available:

I have read and agree to the specifics as stated in the attached policy, which also includes the following:

1. That my use of the e-mail system is for the furthering of the business of this municipality.

2. *That I may not intentionally intercept, eavesdrop, record, read, alter or receive another person's e-mail messages without proper authorization.*

3. *That I may not use the e-mail system for solicitation of funds, political messages or harassing messages.*
4. *That my e-mail messages and data are the property of Middletown and may be accessed for review by supervisors.*

_____ _____

Name *Date*

42.11 Computer Disposal Policy

Disposal of all computer equipment assets will be centrally managed and coordinated by the Information Systems Division. The purpose of this policy is twofold. First, to minimize security risks associated with equipment disposal, by ensuring the secure destruction of discarded data stores. Secondly, computer equipment often contains parts which cannot simply be thrown away. Proper disposal of electronic equipment is both environmentally responsible and is often required by law.

"Computer equipment" refers to desktop, laptop, tablet or netbook computers, printers, copiers, monitors, servers, handheld devices, PDA's, cell phones, disk drives or any storage device, network switches, routers, wireless access points, USB drives, backup tapes or any other backup medium.

When computer equipment assets have reached the end of their useful life, they must be sent to the Information Systems Division for proper disposal. Information Systems will securely erase all storage mediums in accordance with current industry best practices. As an alternative, the hard drives and storage mediums will be removed from each device, and will be rendered unreadable (drilling, crushing, melting down, or other demolition methods).

Computer equipment with non-functioning memory or storage technology will have the memory or storage device removed so that it can be physically destroyed.

Information Systems shall dispose of computer equipment using any authorized method including trade in, reassignment, donation, recycling, refurbishment, sale, or auction. Currently, all surplus computer equipment is auctioned on GovDeals.

Information Systems is not responsible for any loss of data stored on computer equipment. Departments must make copies of any data to be retained before turning the equipment over to Information Systems for disposal. Any City employee found in violation of this policy may be subject to disciplinary action, up to and including termination of employment.

PART B: SOCIAL MEDIA

42.20 Introduction

The prevalence of online social media has made the exchange of information on public or semi-public websites commonplace. To address the new ways that residents communicate and obtain information online, the City has an interest in cultivating and maintaining a positive presence on the Internet in order to reach a broader audience. The City supports the use of social media to further the goals of citizen engagement, where appropriate. Employees are reminded that the use of social media creates public and often permanent records, which may be subject to public records law.

42.21 Purpose

The purpose of this policy is to establish written guidelines concerning the use of social media, social networking, and other forms of Internet-based communication, so that the positive image of the City of Middletown may be maintained and protected.

42.22 Application

A. “Social media”, as used in this policy, is intended to include any material posted on any website, blog, or other medium accessible via the Internet, including but not limited to Facebook, Twitter, and LinkedIn.

B. This policy applies to every City employee, whether part-time or full-time, seasonal or otherwise employed by the City. This policy also applies to all contractors or

temporary employees of the City. The term employee, as used in this policy, means all of these people.

42.23 Policy

A. General

1. The City maintains an online presence. An employee may not characterize himself or herself as representing the City, directly or indirectly, in any online posting unless pursuant to a written policy of the City and at the direction of a supervisor.

2. All social media sites directly or indirectly representing the City must be created pursuant to this policy and must be approved by the City Manager or his/her designee.

3. The City's primary and predominant Internet presence shall remain www.cityofmiddletown.org and no other website, blog, or social media site shall characterize itself as such. Whenever possible, a social media site shall link to or otherwise refer visitors to the City's primary website. In addition to this policy, all social media sites shall comply with all other applicable City policies, including, but not limited to:

   a. Public Records Policy;
   b. Record Retention Policy;
   c. Internet Use Policy;
   d. IT Security Policy; or
   e. Ethics Policy.

4. A social media site is subject to the Ohio Public Records Act and Open Meetings law, and no social media site shall be used to circumvent or otherwise violate any of these laws.

5. Information posted on a social media site will likely be a public record and the City Department posting the information shall maintain an archive of the information and be able to produce it upon request. All official postings on a social media site shall be preserved in accordance with the City's record retention schedules.

6. a. The purpose of social media is to serve as a mechanism for communication between the City and its constituents and all postings are subject to review and deletion by the City. All content posted on a City social media site is owned by the City, and is the exclusive property of the City.

   b. The following kinds of content are not allowed, either by City personnel or by those who post or reply to City social media comments. Such content will be immediately removed and may subject the poster to banishment from all City social media sites.

      i. Comments not topically related to the particular social media article being commented on.
      ii. Comments in support of or in opposition to political campaigns or ballot measures.
      Iii. Profane language or content.
      iv. Content that promotes, fosters, or perpetuates discrimination on the basis of race, creed, color, age, religion, gender, marital status, status with regard to public assistance, national origin, physical or mental disability or sexual orientation.
      v. Sexual content or links to sexual content.
      vi. Solicitations of commerce.
      vii. Conduct or encouragement of illegal activity.
      viii. Information that may tend to compromise the safety or security of the public or public systems.
      ix. Content that violates a legal ownership interest of any other party.

   c. If such content is posted by a City employee, they will be subject to the disciplinary procedures outlined in the policies of the City.

B. City social media sites.

1. For each social media tool approved for use by the City, the following documentation will be developed and adopted:

    a. Operational and use guidelines;
    b. Standards and processes for managing accounts on social media sites;
    c. City and departmental branding standards;
    d. Enterprise-wide design standards; and
    e. Standards for the administration of social media sites.

2. Each City Department that wants to use any form of social media must create a written plan that includes, at a minimum, the following information:

    a. Which social media channels does the department plan to use?
    b. What is the intended purpose and how will social media be used?
    c. What specific topics will be eligible for publishing via social media?
    d. Will two-way communication be allowed, with responses and requests for assistance coming in from the public?
    e. Identify the specific City employees who will be authorized to speak on behalf of the City for this project.
    f. Describe the method that will be used to archive the social media exchanges, so that they can be easily searched, retrieved, and produced for Public Record requests.

3. Every new departmental social media plan shall be routed to the following parties for review and approval:

    a. Information Systems Manager;
    b. Law Director; and
    c. City Manager.

4. The City Manager's Office and the City's Information Systems Division will monitor content on each of the social media sites to ensure adherence to this policy for appropriate use, message, and branding consistent with the mission and values of the City.

The City Manager's Office retains the right to remove information that is inconsistent with the mission of the City.

C. Departmental policies.

1. Individual City Departments may create their own social media policies, as long as they are not inconsistent with the City's social media policy. Departmental policies should be reviewed by the Information Systems Manager to assure compliance with the City policy.

2. It is the responsibility of each City Department to train its employees on the City's social media policy, and any applicable departmental social media policies.

D. Use of non-City social media sites.

1. An employee may not characterize himself or herself as representing the City, directly or indirectly, in any online posting unless pursuant to a written policy of the City or the direction of a supervisor.

2. The intentional, unsolicited and/or unprompted use of a City email address, job title, official City name, seal or logo, shall be deemed an attempt to represent the City in an official capacity. Other communications leading the viewer to conclude that a posting was made in an official capacity shall also be deemed an attempt to represent the City in an official capacity.

3. When posting in a non-official capacity an employee or official shall take reasonable care not to identify themselves as an official or employee of the City. When the identity of an employee or official posting on a non-City social media site is apparent, the employee or official shall clearly state that he or she is posting in a private capacity.

4. Departments have the option of allowing employees to participate in existing social networking sites as part of their job duties. Department Managers may allow or disallow employee participation in any social media activities in their departments.

5. Any postings on a non-City social media site made in an official capacity may be subject to the Ohio Public Records Act and Open Meetings law, and it shall be the responsibility of the employee posting such material to assure that it is maintained as such.

6. An employee or official posting on a social media site shall take reasonable care not to disclose any confidential information in any posting.

7. Employees may engage in the use of private social media during work hours only as is necessary and at a time and in a manner so as not to interfere with the employee's work. City equipment shall not be used for personal use of social media.

8. An employee may not use their City e-mail address to register for a social media site for personal use.

E. Disclaimer language.

If an employee is posting on a social media site for personal purposes or in a private capacity, and the posting in any way identifies the individual as an employee of the City, the posting must contain the following statement:

"The opinion stated herein is the personal opinion of (name of employee) and not the opinion of the City of Middletown or its officials."

PART C: CELLULAR DEVICES (Previously Chapter 26)

42.40 Type of Cellular Device & Service

The determination of whether it is necessary for a City employee to maintain a cellular telephone or other type of cellular device is solely at the discretion of the department director, subject to review by the City Manager if he or she so chooses. City-provided cellular devices or city-reimbursed personal usage of cellular devices, providing data access, must be approved by the City Manager on Form 42A. Upon such determination and approval, when necessary, the employee may choose to have the cellular telephone or device provided by the City or to use their personal cellular telephone or device.

42.41 Devices Provided by City

Cellular devices (telephones, Smartphones, PDA's, etc.) will be provided to employees by the City upon the request of the employee's department director. The device is to be used for business purposes.

A. If the employee uses a city-provided cellular telephone for personal use, the employee will be charged twenty cents ($0.20) for each minute of personal usage within thirty (30) days of the City's receipt of the bill.

B. If the employee uses city-provided data access devices for personal use, the City may, in its sole discretion, discontinue the employee's ability to receive data access and/or discipline the employee.

C. It is the responsibility of the department director (the Chiefs in the case of police and fire) to review the monthly billing statements for City-provided devices to determine that this policy is being followed.

42.42 Use of Personal Cellular Telephones or Other Cellular Devices

A. Employees who are required by the City to have a cellular telephone may use their personal cellular telephone for City purposes. Employees who use their personal cellular telephone for City business under this provision are entitled to a reimbursement by the City of twenty-five dollars ($25.00) per month for each month in which the personal cellular telephone was used for City business, regardless of the amount of usage for City business.

1. Any employee wishing to receive said reimbursement must:

i. Sign an agreement (Form 42B) to keep the device active so long as it is being used for City business; and

ii. Submit an affidavit (Form 42C) by March 15 and September 15 stating the months in which they used their personal cellular telephone for City business and requesting the reimbursement.

2. The reimbursement will be issued two times each year, at the end of March and the end of September. The payment will be at the discretion of the department director, and is subject to budgetary limitations.

B. Employees who are required to maintain data access on a cellular device may use their personal cellular device for City purposes. Employees who choose to do so on a personal cellular device under this provision are entitled to a reimbursement by the City of thirty dollars ($30.00) per month. All reimbursements are at the discretion of the department director and subject to budgetary limitations.

1. Any employee wishing to receive such reimbursement must:

i. Submit and have approved Form 42A, an approval of cellular data access, by the City Manager;

ii. Sign an agreement (Form 42B) to keep the device active so long as it is being used for City business; and

iii. Submit an affidavit (Form 42C) by March 15 and September 15 stating the months in which the personal cellular telephone was used for City business and requesting the reimbursement.

2. The reimbursement will be issued two times each year, at the end of March and the end of September. The payment will be at the discretion of the department director, and is subject to budgetary limitations.

42.43 Duties

A. The department director (Chiefs for police and fire) shall maintain an accurate list of all telephone numbers for the cellular devices of employees in their department required to maintain a cellular telephone or other cellular device.

B. If an employee is required by the City to have a cellular device, and the employee elects to use a personal device,

the employee shall be subject to disciplinary action for failure to maintain active service on their personal device.

FORM 42A

City of Middletown
Approval of Data Access on a Cellular Device

Name _____

Department _____

Title _____

Reason for data access:

_____

_____

_____

_____

_____

_____ _____
Department Director City Manager

Date _____ Date _____

Form 42B

City of Middletown
Cell Phone Reimbursement Signup

Name _____

Department _____

Replace City Cell phone: Yes No

City Cell Number _____

Personal Cell Number _____

I agree to maintain my personal phone account during the entire time I will be requesting reimbursement. I also agree to notify my department head of any changes in availability or if my personal phone number changes.

Signature _____ Effective Date _____

Form 42C

City of Middletown
Cell Phone Reimbursement Affidavit

Name _____

Department _____

Personal Cell Number _____

Number of Months reimbursement _____

I hereby certify that I have kept my personal cell phone account active during the period of time I am requesting reimbursement. Access to this number must be maintained throughout the entire period. Any changes to availability must be reported immediately to my department head. Failure to report changes in phone numbers, or requesting reimbursement for ineligible time may result in disciplinary action up to dismissal.

I am requesting reimbursement for the following cellular services:

Voice ☐ Data ☐

Signature _____ Date _____