ALLITHWAITE AND CARTMEL PARISH COUNCIL

COMMUNICATION AND INTERNET SECURITY - POLICY AND PROCEDURE FOR COUNCILLORS

APPROVED AND ADOPTED: 11th July 2024.
TO BE REVIEWED: June 2025 and annually thereafter.

SUMMARY

Allithwaite and Cartmel Parish Council (the Council) provides employees and councillors with access to various computer facilities for work and communication purposes. In order to ensure compliance with all applicable laws in relation to data protection, information security and compliance monitoring, the council has adopted an IT communications, security and monitoring policy which should be read in conjunction with its' Data Protection policy.

This document is in three parts covering:

Part 1 - Email and the Internet – pages 4 - 7
Part 2 - Electronic Commications – pages 9 - 13
Part 3 - IT Security – pages 15 - 19

Allithwaite and Cartmel PC (ACPC) makes use of IT systems, for data storage, communications and as a source of information in order to:

- prevent inappropriate use of computer equipment (such as extended personal use or for accessing and circulating pornographic, racist, sexist or defamatory material)
- protect confidential, personal or commercially sensitive data
- prevent the introduction of viruses
- prevent the use of unlicensed software
- ensure that Council property is properly looked after
- monitor the use of computer facilities to ensure compliance with internal policies and rules and to detect abuse

Breach of this policy will be regarded as a disciplinary offence and will be dealt with under the Council's disciplinary process.

Anyone who considers that there has been a breach of this policy in relation to personal information about them held by the Council should raise the matter via the Council's formal complaint procedure.

PART 1 – EMAIL AND THE INTERNET

CONTENTS: **PAGE**

1. INTRODUCTION

Allithwaite and Cartmel Parish Council ("the Council") provides email facilities for use by Councillors who have access to a desktop, laptops or mobile devices. This document sets out the Council's policy for the use of these services and more general computer use in compliance with the General Data Protection Regulations (GDPR).

2. OBJECTIVES

The objectives of the policy are to ensure that the services made available to Councillors are used:

- In accordance with the values, principles and standards of the Council.
- Ensure GDPR is complied with by ensuring only Allithwaite and Cartmel Parish.
- Council approved email accounts are used for council business.
- So as not to incur legal liability.
- So as not to threaten the integrity of the Council's IT services.

3. ACCEPTANCE OF THE POLICY

The policy applies to all Allithwaite and Cartmel Parish Council Councillors. All Councillors are required to sign to indicate their acceptance of the policy Appendix 1) content at the time of joining the Council and will be asked to re-affirm their understanding and acceptance of the policy on an annual basis.

Each Councillor is responsible for individually complying with this policy.

4. SECURITY

Access to the Councillors network and files, including Internet services, is restricted to individual users and MUST not be shared accounts.

- The access of each user is controlled by means of their own password.
- Passwords must be kept confidential and not disclosed to others; disclosure could result in Internet or email misuse being attributed to the owner of the password.
- Guidance on password protection of files is available from the Clerk to the Council.
- Care should be taken not to leave a device that is connected to the Internet/system unattended or unlocked.
- Breaches of security of the computer system e.g. disclosure of personal passwords, giving unauthorised access to emails to external parties, may result in action from the Information Commissioners Office (ICO).
- For further protection of personal data, all files containing names, telephone numbers, addresses and email addresses, etc. must be password protected. These files are likely to take the form of internal databases, registers etc.
- If you suspect there has been data breach or your email/IT has been hacked, you must inform the Clerk immediately. The Clerk will then report this breach to the Council's Data Protection Officer for guidance on the most appropriate way to deal with the breach.

5. GUIDANCE

This section of the document provides guidance on the acceptable use of the Council's email and Internet services and contacts databases.

5.1 Email Usage

The Council's email system enables users to email Officers and Members of the Council, as well as individuals outside of the organisation. Users should be aware that once an email is sent to an

individual outside of the Council, it is beyond the Council's control and is not guaranteed to be confidential.

5.2 Hoax / Suspect Emails

Hoax and/or suspect emails should be reported to the Clerk. They should not be opened or forwarded but "double deleted" i.e. deleted from the users "Inbox" and then "Deleted Items".

5.3 Prohibited Email Activities:

The following email activities may breach the councils 'code of conduct' and/or prompt action by the Information Commissioners Office:

- Examining, changing or using another person's files, output or user name without explicit authorisation.
- Sending or forwarding any material that is obscene, defamatory or hateful, or which is intended to annoy, harass or intimidate others.
- Sending or forwarding emails which are likely to damage the reputation of the Council
- Sending or forwarding electronic chain letters.
- Soliciting emails that are unrelated to Council activities or soliciting non-Council business for personal gain or profit.
- Intentionally interfering with the normal operation of the Council's network, including the propagation of computer viruses and the generation of sustained high-volume network traffic
- Sending or forwarding attachments of such size or arrangement as to cause disruption to the Council's network.

5.4 Personal Email Use

The use of Allithwaite and Cartmel Parish Council email for personal purposes is not permitted.

5.5 Email Awareness

Email is not a secure method of transmission - it should not be assumed that any email communication is secure or private. Users should take this into account particularly when emailing confidential or sensitive information.

5.6 Email Best Practice

- Ensure that each email has a specific target audience.
- Be selective, especially when deciding who should be copied in on an email. This ensures that only those who really require the information receive it and avoids wasteful emails and wasted time/resources.
- If you are copying in a recipient(s) who you think have not given permission for their email to be circulated use Bcc to protect their information
- The circulation of emails with attachments to large groups should be avoided
- When sending emails to a large number of people the recipients' addresses should be entered into the BCC (blind copy) field. Users should contact the Council's Parish Clerk or Webmaster if assistance is required
- Emails should not be kept in separate folders in an individual's folder list longer than is necessary, if at all.
- Time should be set aside on a regular basis for "housekeeping", in order to delete old or unwanted items from mailboxes. This is essential in order to ensure the efficient operation of the email system and helps to keep mailboxes organised and ensure that councils GDPR retention policy is complied with.
- The 'Inbox', 'Sent Items' and 'Deleted Items' folders should be examined as part of a housekeeping routine, performed at a minimum frequency of once a month. Contact the

council's Parish Clerk or Webmaster for assistance if you are unsure of how to complete any of the processes described in this policy.

5.7 Email Etiquette

Email is all about communication with other people, and as such some basic courtesy should be observed:

- Always include a subject line in your message.
- When replying to an email, include enough of the original message to provide a context.
- An email signature is a good way of providing detail of who is sending the email, and the details of how to respond.
- Consider the tone and language used, and the use of plain English. When sent externally emails represent and reflect upon the Council.
- Avoid using capitals throughout as this is equivalent to shouting.

5.8 Database Usage

In accordance with the Data Protection Act, no personal details/data from any contacts databases e.g. Parish Council Contacts, should be given out to external parties at any time.

No personal data/databases should be kept on any storage facility e.g. CD's, DVD's 3 1 /4" discs, USB's laptops or personal home-based computers, as this could result in legal action from third parties.

Any communication by a councillor that is not associated directly with Allithwaite and Cartmel Parish Council business (ie: it is carried out by a councillor acting on their own by or on behalf of another) is not considered as acting as a councillor by the ICO 'the business of the council'.

Therefore, you are not covered by the council's data protection fee requirement to the Information Commissioners Office https://ico.orq.uk/fororganisations/data-protection-fee/ and as such you will be responsible (as an individual) for complying with ALL the General Data Protection Regulations regarding data security.

6. ACCESS CONTROL AND MONITORING

The following will apply when the services are accessed from the Council's network.

6.1 Email Monitoring

The Council has the ability to monitor email activity, so that compliance with this policy and other relevant policies and regulations can be effectively managed.

6.2 Email Viruses

Continuous virus checking of all incoming email will take place. However, it is possible that a new virus may not be detected by the Council's virus scanner and users should be wary of opening attachments to emails from an unknown source; in particular attachments with names ending in "exe" should not be opened. If you receive notification of a virus via chain email do not forward to anyone. Advise the Clerk who will then notify the Parish Clerk or Webmaster of the details who will investigate the virus threat.

Section 5.1 gives additional information on dealing with hoax/suspect emails.

This policy will be reviewed every two years or when new legislation is introduced.

ALLITHWAITE AND CARTMEL PARISH COUNCIL **APPENDIX 1**

Email, Internet and Computer System Use Policy - ACCEPTANCE SLIP

I have received, read and understood the Council's Email, Internet and Computer Use Policy.

I understand that:

- My use of Allithwaite and Cartmel Parish Council email will be monitored for management and security purposes.
- If I use my own computer/laptop/tablet for council business I confirm I am responsible for ensuring I comply with IT security and data protection as required under the General Data Protection Regulations.
- Breaches of the policy may result in action being taken against me by the Information Commissioners Office.

Signed _____

Name _____

Date _____

PART 2 – ELECTRONIC COMMUNICATIONS AND EMAIL

CONTENTS **PAGE**

1. INTRODUCTION

This policy is introduced to provide guidelines as to the use of the website and electronic communications within Allithwaite and Cartmel Parish Council (A&CPC), between councillors and employees, and between A&CPC and the public. Electronic communications may include emails, text messaging on any platform, and social media. The policy complies with all relevant legislation including the General Data Protection Regulation (GDPR) legislation 25 May 2018.

Allithwaite and Cartmel Parish Council recognises email as a valuable communications tool that adds to other communication channels and encourages its use by elected members and staff.

It provides email addresses for the use of Councillors and staff. It will provide computer equipment and consider requests by Councillors for assistance in training in use of new technology.

2. STATEMENT OF POLICY

The purpose of this policy is to set out the procedure for administration of the A&CPC website (www.allithwaiteandcartmel-pc.gov.uk) and general electronic communications with members of the public. The Parish Council welcomes the opportunity to communicate with residents and members of the public and understands that it plays an important role in the democratic process.

The website, emails and social media can be useful conduits for promoting the Parish Council and ensuring that residents are aware of Parish Council initiatives. A good working relationship can be highly positive and should be regarded as a desirable outcome of Parish Council communications. The website, email, messaging and social media platforms are also essential communications tools used to carry out the business of A&CPC.

All councillors and council employees communicating on behalf of A&CPC must ensure that their use of these tools is appropriate and lawful and will not damage the reputation of the Council or its employees, or otherwise infringe any of the Council's policies.

3. PURPOSE OF THE PARISH COUNCIL WEBSITE

The Allithwaite and Cartmel website provides essential information about the Parish Council to the public, including:

- General description of the purpose and activities of the Parish Council
- Details of the parish councillors and their registers of interests
- Contact details of the Clerk including address, email and phone number
- Financial information
- Policies and Procedures
- Details of Parish Council Meetings together with agendas and minutes
- Historical minutes of the Parish Council and Annual Parish Meetings if available
- The Allithwaite and Cartmel Neighbourhood Plan and other information on Planning in Allithwaite and Cartmel.
- Grants available to the Allithwaite and Cartmel community
- Local facilities, Newsletters
- News and events of interest to Allithwaite and Cartmel residents

4. ADMINISTERING THE ALLITHWAITE AND CARTMEL WEBSITE

All news and information posted on the Allithwaite and Cartmel website is authorised by the Clerk and/or the Chairman. Other parish councillors may be given delegated authority by the Clerk or Chairman to post news or information in their area of knowledge or interest.

The Clerk has primary responsibility for administering the website and may also authorise parish councillors to carry out website administration on their behalf.

Requests from any organisation to publish information on the Allithwaite and Cartmel website are considered on a case-by-case basis. Allithwaite and Cartmel will endeavour to publish news and information which will be helpful to Allithwaite and Cartmel residents.

5. USE OF EMAIL AND TEXT MESSAGING

All councillors and employees of the council emailing on behalf of the council must use email and text messaging responsibly.

Text messaging includes the use of electronic communication platforms such as WhatsApp and Messenger.

The term 'email' is used in the following to include these forms of text messaging as well.

Responsible use of email means:

- Email correspondence should be undertaken in a professional and responsible manner respecting personal privacy and the requirements of data protection legislation;
- Those writing or replying to emails should check to see that the email is only being copied to the person or persons intended; and that there is no sensitive information contained in any attached document or any accompanying email 'trail', that is, previous emails attached to the email being sent;
- Sensitive or confidential parish council information is not sent or copied to people outside the council; if you are unsure consult the Clerk;
- Where emails are sent which contain personal details the personal details should be limited to that information which is required for the business of the council;
- If inappropriate material is sent accidentally this must be reported immediately to the Clerk or Chairman, or the Vice Chairman in the absence of the Chairman;
- Emails must not contain inappropriate or unlawful material, which includes, but is not limited to,: abusive, threatening, sexual, discriminatory, racial, obscene or hate text or images.
- Parish councillors and employees should make use of the specific council email address '…@allithwaiteandcartmel-pc.gov.uk' for all email communication concerning Parish Council business, unless technical difficulties make this impossible

If you are unsure about anything above, please consult the Clerk who can advise on email etiquette.

Emails broadcast to mailing lists on behalf of the Parish Council must be authorised by the Clerk and/or Chairman, who may give delegated authorisation to other parish councillors.

6. USING EMAIL EFFECTIVELY

- Do not assume privacy for any Internet communications of any kind. E-mails and/or files can be posted or forwarded to other Internet users around the world without the user's knowledge or permission.

- Defamatory, libellous, abusive, sexist or racist comments in e-mail may render the sender personally liable to civil action.

- Any messages or information sent by an Employee or Member are statements that reflect the Council. All Users should be aware that their views will be construed as representing the Council. Users should include a disclaimer with their email stating that 'the views expressed are personal and may not necessarily reflect those of the Parish Council, unless explicitly stated otherwise.

- Members using their private or business email addresses should clearly distinguish Parish Council emails from their own emails when corresponding with third parties on behalf of the Parish Council. Guidance on creation of standard electronic signatures can be provided. It should be noted that a disclaimer does not legally divorce the legal connection between the sender and the Council.

The following procedures are recommended practice:

DO:

- Consider whether e-mail is the best way to send a message; Messages may not be secure.
- Messages may not be read immediately.
- Don't assume that they have been read! messages may be produced as proof that you said something.
- Messages may be held to be legally binding.
- Messages may be subject to tampering after delivery or sending. Messages can be edited!
- Messages may continue to exist after you think you have deleted them. Never assume that deleted items can't be retrieved!
- Apply the same principles you would use with a printed memo; Content should be clear and not open to misinterpretation.
- Use plain English Include a meaningful and logical subject line. If the recipient is not expecting the e-mail and does not recognise the subject of the data they may delete it. Always ring the recipient if they are not expecting something unusual.

    - ✓ Include your position and contact details the first time you correspond. Use standard fonts and effects to ensure legibility.
    - ✓ Only copy to those who need a copy.
    - ✓ If you are transmitting sensitive data, send it in a password protected document.

- Make it clear to recipients why you are sending an email, especially circular emails. Is it for information only, or do you expect a reply? Is it a request for a specific piece of information, or are you seeking opinion?
- Check incoming mail regularly and respond promptly.
- Do not save attachments in your email file. Save them to a logical location in your work area

DON'T

- Use e-mail to avoid difficult face-to-face communication.
- Use email for dialogue which would better be held in meetings or get into "tit for tat" interchanges.
- Use e-mail to send confidential information. If you have to use email send your correspondence in an attached word file with password protection.
- Use e-mail to send personal information without authorisation.
- Send messages that may be read as obscene, harassing, intimidating or discriminatory.

- Send messages in anger, even in response to abusive mail.
- Send messages in CAPITALS – it may be interpreted as shouting.
- Send messages to "everyone" or "reply all" without checking whether it is relevant and appropriate to do so.
- Forward or respond to junk mail, chain letters, virus hoaxes, etc.

7. USE OF SOCIAL MEDIA

The aim of this section of the policy is to set out a Code of Practice to provide guidance to parish councillors and employees of Allithwaite and Cartmel in the use of online communications, collectively referred to as social media.

Social media is a collective term used to describe methods of publishing on the internet. The policy covers all forms of social media and social networking sites which include (but are not limited to):

- Facebook
- X (formerly Twitter)
- Myspace and other social networking sites
- Blogs and comments on other websites
- Online chatrooms and forums
- YouTube and other video clips and podcast sites
- LinkedIn

8. CODE OF CONDUCT FOR USE OF SOCIAL MEDIA

Individual parish councillors are responsible for what they post. Councillors are personally responsible for any online activity conducted via their social media accounts or through interaction with other online sites and forums.

When participating in any online communication on a council matter, councillors and employees should:

- Be responsible and respectful; be direct, informative, brief and transparent.
- Always disclose your identity and affiliation to the Parish Council.
- Never make false or misleading statements.
- Not present themselves in a way that might cause embarrassment.
- Be mindful of the information they post on sites and make sure personal opinions are not published as being that of the Council or bring the Council into disrepute or is contrary to the Council's Code of Conduct or any other Policies.
- Keep the tone of your comments respectful and informative.
- Councillors should refrain from personal criticism in social media of other councillors and individuals or organisations with whom the Parish Council has dealings (in accordance with the Nolan principles of conduct in public life)
- Language that may be deemed as offensive relating to race, sexuality, disability, gender, age or religion or belief should not be published on any social media site.
- Avoid personal attacks, online fights and hostile communications.
- Permission to publish photographs or videos on social media sites should be sought from the persons or organisations in the video or photograph before being uploaded.
- Respect the privacy of other councillors, employees and residents.
- Do not post any information or conduct any online activity that may violate laws or regulations (for example, copyright laws see below) Councillors and employees should be aware that:
- Posting copyright images or text on social media sites is an offence. Breach of copyright may result in an award of damages against you.

- Publishing personal data of individuals without permission is a breach of Data Protection legislation is an offence.
- Publication of obscene material is a criminal offence and is subject to a custodial sentence.
- Councillors views posted in any capacity in advance of matters to be debated by the council at a council meeting may constitute Pre-disposition, Predetermination or Bias and will require the individual to declare an interest at council meetings.

Allithwaite and Cartmel will use all reasonable efforts to ensure that use of social media in connection with its business by councillors, employees and members of the public are within the law. It cannot be held responsible for damages resulting from the misuse of social media in a way contrary to this policy.

9. MONITORING SOCIAL MEDIA USE

The clerk will monitor social media accounts and sites controlled by Allithwaite and Cartmel however the diverse nature of social media means that it is nearly impossible for one person to continually monitor and review activity by councillors on social media.

Councillors are therefore responsible for their own use of the media and will be held accountable where breaches are brought to the attention of Allithwaite and Cartmel Parish Council. In such instances they will be considered as any other breach of the Code of Conduct for Councillors would be.

PART 3 – INTERNET SECURITY

CONTENTS **PAGE**

1. INTRODCUTION

ACPC provides you with access to various computing and telephone communication methods to allow you to undertake the responsibilities of your position and to improve internal and external communication.

This policy sets out the Council's position on your use of the Facilities and it includes:

- your responsibilities and potential liability when using the Facilities;
- the monitoring policies adopted by the Council; and guidance on how to use the Facilities.

2. THIS POLICY HAS BEEN CREATED TO:

- ensure compliance with all applicable laws relating to data protection, information security and compliance monitoring;
- protect the Council from the risk of financial loss, loss of reputation or libel;
- ensure that the equipment is not used so as to cause harm or damage to any person or organisation.

3. THIS POLICY APPLIES TO THE USE OF:

- local, inter-office, national and international, private or public networks and all systems and services accessed through those networks;
- desktop, portable and mobile computers and applications;
- social media;
- electronic mail and messaging services.

4. COMPUTER FACILITIES: USE OF COMPUTER SYSTEMS

Subject to anything to the contrary in this policy the equipment must be used for Council business purposes only.

In order to maintain the confidentiality of information held on or transferred via the Council's equipment, security measures are in place and must be followed at all times. A log-on ID and password is required for access to the Council's equipment/network. This will be changed regularly and must be kept secure and not shared with anyone. A full list of account details should be held with the clerk in a sealed secure unit.

You are expressly prohibited from using the equipment for the sending, receiving, printing or otherwise disseminating information which is the confidential information of the Council or its clients other than in the normal and proper course of carrying out your duties for the Council.

In order to ensure proper use of Council computers, you must adhere to the following practices:

- anti-virus software must be kept running at all times;
- media storage such as USB drives, CD's or portable hard drives will not be permitted unless they have been provided by the IT supplier or approved by Council;
- obvious passwords such as birthdays and spouse names, etc, must be avoided (the most secure passwords are random combinations of letters and numbers);
- all files must be stored on the network/computer cloud drive which is backed up regularly to avoid loss of information;
- always log off the computer/network before leaving your computer for long periods of time or overnight.

5. SOFTWARE

Software piracy could expose both the Council and the user to allegations of intellectual property infringement. The Council is committed to following the terms of all software licences to which the Council is a contracting party. This means, that:

- software must not be installed onto any of the Council's computers unless this has been approved in advance by our IT Contractors or Council. They will be responsible for establishing that the appropriate licence has been obtained, that the software is virus free and compatible with the computer facilities;
- software should not be removed from any computer nor should it be copied or loaded on to any computer without prior consent.

6. LAPTOP COMPUTERS, PC'S, TABLETS AND SMART PHONES

Laptop computers, PC's, tablets and smart phones belonging to the Council along with related equipment and software are subject to all of the Council's policies and guidelines governing non-portable computers and software. All laptops, PC's and tablets will be encrypted. When using such equipment:

- you are responsible for all equipment and software until you return it. It must be kept secure at all times;

- The clerk and the individual staff members are the only person authorised to use the equipment and software issued to you;

- you must work within the Councils filing/software environment when carrying out Council business to ensure that all data is backed up and accessible by the Clerk;

- if you discover any mechanical, electronic, or software defects or malfunctions, you should immediately bring such defects or malfunctions to the Council's attention;

- upon the request of the Council at any time, for any reason, you will immediately return any equipment and all software to the Council;

- if you are using your own laptop or PC to connect with the Council's network or to transfer data between the laptop or PC and any of the Council's computers you must ensure that you have obtained prior consent, comply with instructions and ensure that any data downloaded or uploaded is free from viruses.

7. EMAIL (INTERNAL OR EXTERNAL USE)

All Cllrs & Staff will be issued a Council email account which must always be used when transacting on behalf of the PC.

Internet email is not a secure medium of communication; it can be intercepted and read. Do not use it to say anything you would not wish to be made public. If you are sending confidential information by email this should be sent using password protected attachments.

Email should be treated as any other documentation. If you would normally retain a certain document in hard copy you should retain the email.

Do not forward email messages unless the original sender is aware that the message may be forwarded. If you would not have forwarded a copy of a paper memo with the same information do not forward the email.

Your email inbox should be checked on a regular basis.

As with many other records, email may be subject to discovery in litigation. Like all communications, you should not say anything that might appear inappropriate or that might be misinterpreted by a reader.

Viewing, displaying, storing (including data held in RAM or cache) or disseminating materials (including text and images) that could be considered to be obscene, racist, sexist, or otherwise offensive may constitute harassment and such use of the Facilities is strictly prohibited.

The legal focus in a harassment case is the impact of the allegedly harassing material on the person viewing it, not how the material is viewed by the person sending or displaying it.

Staff will be required to surrender their email account and all of its contents to the Clerk if they decide to leave the Council.

8. INTERNET

Posting information on the internet, whether on a newsgroup, via a chat room or via email is no different from publishing information in the newspaper. Staff should confirm the posting with the Clerk prior to issue.

Using the internet for the purpose of trading or carrying out any business activity other than Council business is strictly prohibited.

For the avoidance of doubt the matters set out above include use of wireless facilities.

9. MONITORING POLICY

The policy of the Council is that we may monitor your use of the equipment.

The Council recognises the importance of an individual's privacy but needs to balance this against the requirement to protect others and preserve the integrity and functionality of the equipment.

The Council may from time to time monitor the equipment. Principal reasons for this are to:

- detect any harassment or inappropriate behaviour by employees, ensuring compliance with contracts of employment and relevant policies including the health and safety, ethical and sex discrimination policies;
- ensure compliance of this policy;
- detect and enforce the integrity of the Facilities and any sensitive or confidential information belonging to or under the control of the Council;
- ensure compliance by users of the Facilities with all applicable laws (including data protection), regulations and guidelines published and in force from time to time;
- monitor and protect the wellbeing of employees.

The Council may adopt at any time a number of methods to monitor use of the Facilities. These may include:

- recording and logging of internal, inter-office and external telephone calls made or received by employees using its telephone network (including where possible mobile telephones). Such recording may include details of length, date and content;
- recording and logging the activities by individual users of the Facilities. This may include opening emails and their attachments, monitoring Internet usage including time spent on the internet and websites visited;
- physical inspections of individual users computers, software and telephone messaging services;
- periodic monitoring of the Facilities through third party software including real time inspections;
- physical inspection of an individual's post;
- archiving of any information obtained from the above including emails, telephone call logs and Internet downloads.

The Council will not (unless required by law):

- allow third parties to monitor the Facilities (with the exception of our appointed IT supplier); or

- disclose information obtained by such monitoring of the Facilities to third parties unless the law permits.

The Council may be prohibited by law from notifying employees using the equipment of a disclosure to third parties.

10. SOCIAL MEDIA

The Council may use social media to communicate messages to residents and will only be used:

- by the Clerk and persons nominated by the Clerk;
- to transmit factual information and news, not personal opinion;
- to respond to comments and requests submitted via the account.

Staff using their own social media accounts must ensure that any comment made is clearly identified as their own and not representative of the Council.

11. GENERAL GUIDANCE

Never leave any equipment or data (including client files, laptops, computer equipment and mobile phones) unattended on public transport or in an unattended vehicle.

–