COLL COMMUNITY COUNCIL

Digital Communications, Social Media, Data Protection and Artificial Intelligence Policy

Easy-Use Guide and Formal Policy
Version 1.5 - Final Draft for Adoption

Compatibility review: 2 October 2026 - cross-checked against CCC Privacy Notice 2025 and current Processing/Retention Register.

Status	Final draft for formal adoption by Coll Community Council
Applies to	CCC members, office bearers, official subcommittees and working groups
Policy owner	Coll Community Council
Review	Annually, or sooner following significant legal, ICO, Argyll and Bute guidance or technology changes

PART A - QUICK GUIDE FOR CCC MEMBERS

1. Why we have this policy

Coll Community Council (CCC) needs to communicate effectively with residents, organisations, public authorities and one another. WhatsApp, email, Facebook, Instagram and artificial intelligence can all make this easier, but they can also create risks if personal, confidential or sensitive information is used inappropriately.

This policy is intended to make those responsibilities easier to understand and follow. CCC recognises that Community Councillors are volunteers and are not expected to be experts in data-protection law, information governance, social media, cyber security or artificial intelligence.

The policy is designed to align with applicable UK data-protection requirements, Information Commissioner's Office (ICO) guidance and relevant Argyll and Bute Council Community Council guidance.

2. The rule to remember

Use the minimum information necessary.

Share it only with people who reasonably need it.

Protect private, confidential and sensitive information.

If genuinely unsure - ask before sharing.

3. Traffic-light guide

Level	Practical rule and examples
GREEN - NORMALLY OK	Public or routine information: published agendas/minutes, meeting notices, ferry or transport information, public consultations, public funding opportunities, links, newsletters, ordinary administration, appropriate public posts, and AI used for general research or non-confidential drafting. Normally proceed using reasonable judgement. Quick link: Section 23A - Public information and AI
AMBER - STOP AND THINK	Names of residents, personal correspondence, complaints, identifiable photographs, telephone numbers, personal email addresses, privately supplied information, disputes, unpublished correspondence, uncertain information, or identifiable information being considered for AI. Use only what is needed; remove identifiers where possible; ask if uncertain.

© Coll Community Council 2026

	Quick links: Section 8 - Personal information | Section 9 - Data minimisation | Section 17 - Complaints
RED - STOP AND SEEK ADVICE	Medical/health information, bank details, passwords, security information, highly sensitive personal information, confidential legal advice, confidential complaints containing unnecessary personal data, serious unverified allegations, confidential material on public social media, inappropriate sensitive WhatsApp sharing, or unnecessary confidential/sensitive data entered into public AI. Quick links: Section 19 - Information not for public AI | Section 25 - Data breaches

Unsure which level applies? Go to Section 4 - The five-question test

4. The five-question test

1. Is this legitimate CCC business?
2. Do I actually need to use or share this information?
3. Is it personal, private, sensitive or confidential?
4. Do the people receiving it reasonably need to see it?
5. Would I be comfortable if it were forwarded, copied or screenshotted?

If genuinely uncertain - don't guess. Ask.

AI CAN ALSO HELP YOU CHECK

You may use AI to help understand this policy, identify possible GREEN / AMBER / RED issues, or prepare documents from legitimate public information. Anonymise where necessary, do not enter unnecessary confidential or sensitive personal information, check important outputs, and seek human advice if a serious issue remains uncertain.

PART B - FORMAL POLICY

5. Purpose and scope

This policy establishes practical rules for CCC's use of WhatsApp and other messaging applications; Facebook, Instagram and other social media; email; websites and online forums; cloud-based services; photographs, video and audio; electronic records; generative artificial intelligence systems such as ChatGPT, Microsoft Copilot, Google Gemini and similar services; and future digital communication technologies.

The objective is to enable CCC to communicate effectively while protecting personal information, maintaining confidentiality and supporting good governance.

VERIFIED GOVERNANCE BASIS

This policy has been developed with reference to applicable legislation, ICO guidance and the current Argyll and Bute Community Council framework. Full sources are listed in section 31.

6. Relationship with Argyll and Bute Council

This is Coll Community Council's own policy. It has been developed having regard to relevant Argyll and Bute Council Community Council guidance and, as good-practice reference material, relevant approaches to data protection, ICT acceptable use and social media.

Adoption of this policy does not mean that Argyll and Bute Council's corporate ICT Acceptable Use Policy previously applied automatically to CCC or its members. CCC is establishing its own rules appropriate to a Community Council.

This policy applies prospectively from the date on which CCC formally adopts it. It should not normally be applied retrospectively to conduct occurring before that date.

© Coll Community Council 2026

7. Safe-working principle for members

CCC recognises that its members are volunteers. Members cannot reasonably be expected to be experts in data-protection law, information governance, cyber security, social media or artificial intelligence.

CCC expects members to act reasonably and in good faith; follow this policy; use the minimum personal information reasonably necessary; protect confidential and sensitive information; use reasonable judgement; and seek advice where genuinely uncertain.

A member who follows these principles will normally be regarded by CCC as having followed the expected standard of conduct. This does not remove CCC's or an individual's obligations under applicable law. Seeking advice is good governance and is not an admission that a member has done something wrong.

7A. CCC as data controller and lead responsibility

Argyll and Bute Council's current Community Council data-protection information states that community councils are data controllers and should have a named person with lead responsibility for data-protection compliance.

- CCC should maintain any ICO registration or data-protection fee arrangements that are legally required.
- CCC should nominate an office bearer or other appropriate member as its data-protection lead/contact.
- The nominated contact provides a clear point of contact, but responsibility for lawful handling of information remains with CCC and with members carrying out CCC duties.
- Where a member is unsure whether a matter requires specialist advice or ICO contact, it should be referred promptly to the nominated lead.

This section is intended to make responsibility clear without expecting the nominated member to act as a professional data-protection officer.

8. Personal information

Personal information can include names, addresses, telephone numbers, email addresses, photographs, correspondence, complaints, opinions about identifiable individuals and combinations of information from which an individual can reasonably be identified.

Particular care must be taken with more sensitive information, including health information and other special-category personal data. Receiving information does not automatically mean that a member is entitled to redistribute it.

Core rule: if personal information is not reasonably needed, do not collect it, copy it, forward it, upload it or retain it.

9. Lawfulness, purpose and data minimisation

Where CCC processes personal information it must have a valid lawful basis and handle the information lawfully, fairly and transparently. The appropriate basis depends on the purpose and circumstances. Where special-category personal data is processed, CCC must also identify an appropriate additional condition for that processing. Members are not expected to determine complex lawful-basis questions unaided; uncertain or higher-risk cases should be referred for advice.

CCC's Privacy Notice currently identifies public task as the lawful basis for its core Community Council functions. CCC's Register of Processing Activities and Privacy Notice should be reviewed together and kept consistent as to the lawful basis relied upon for each processing purpose. Where a different lawful basis is appropriate for a particular activity, that basis should be identified and documented.

Only the minimum information reasonably necessary for legitimate CCC business should be used. Where appropriate, information should be anonymised or redacted before wider circulation.

10. WhatsApp and other messaging services

WhatsApp and similar services may be useful for alerts, routine administration, meeting reminders, transport information, links, consultations, public funding information, public notices and other routine information-sharing.

They should not normally be used for highly confidential CCC business, sensitive personal information, confidential complaints, unnecessary detailed discussion about identifiable individuals or confidential documents containing personal information. WhatsApp must not be used as a substitute for formal CCC decision-making.

Members should remember that messages can be copied, forwarded and screenshotted.

© Coll Community Council 2026

11. Official WhatsApp or messaging groups

An official CCC, subcommittee or working-group messaging group should have a reasonably clear purpose, appropriate administrators and membership relevant to that purpose. Membership should be periodically reviewed and former participants removed where appropriate.

Participants should understand who is in the group and the nature of the group. Important CCC business should be transferred to appropriate official records where necessary.

12. Facebook, Instagram and other social media

Official CCC social-media accounts may advertise meetings, publish public information, promote consultations, distribute notices, communicate CCC activities and encourage community engagement.

Official accounts should not publish confidential information, unnecessary or sensitive personal information, unverified allegations, defamatory, abusive, threatening or discriminatory material, confidential complaints or material otherwise inconsistent with CCC's governance responsibilities.

13. Personal social-media accounts

Community Councillors may use personal social-media accounts, but conduct connected with their CCC role may still engage the relevant standards of conduct.

Official CCC communications and authority to speak

When communicating an official CCC view in writing, on social media, by email, through messaging services, to the media or to another organisation, a member should ensure that they have appropriate authority from CCC to do so.

- Where CCC has formally agreed a position, an authorised member may communicate that agreed position accurately.
- Where CCC has not agreed a position, a member should make clear that they are expressing a personal view or providing information rather than speaking on behalf of CCC.
- Routine administrative communications within an office bearer's or member's agreed role do not require a separate formal decision each time, provided the communication remains within that authority.
- Where there is genuine doubt about whether a member is authorised to communicate a CCC position, the member should check with the Convenor, Secretary or CCC before presenting the communication as an official CCC view.

14. Management of official accounts and security

Where reasonably practicable, more than one authorised person should have appropriate access to important CCC digital accounts. Passwords should be secure, not unnecessarily shared and changed when appropriate. Access should be removed when no longer required. Multi-factor authentication should be used where reasonably available and appropriate.

Members should protect devices, take appropriate care with public Wi-Fi, protect confidential documents and promptly report lost devices containing significant CCC information.

15. Email

Before sending CCC email, members should check recipients; consider BCC where recipients do not need to see one another's addresses; avoid unnecessary 'Reply All'; remove unnecessary personal information; consider whether previous correspondence needs to remain attached; and avoid distributing confidential information more widely than necessary.

CCC business should, where reasonably practicable, be distinguishable from unrelated personal correspondence.

16. Photographs, video and audio

Photographs, video and audio may contain personal information where individuals can be identified.

Members should consider why the material is required, whether people would reasonably expect the use, where it will be published, whether children or vulnerable individuals are identifiable, whether consent or another appropriate basis is required, and how long it needs to be retained.

© Coll Community Council 2026

17. Complaints and correspondence

Complaints and correspondence involving identifiable individuals should only be circulated to those who reasonably need the information for CCC purposes. Where appropriate, information should be summarised, redacted or anonymised.

Publication of CCC agendas or minutes should not automatically result in publication of unnecessary personal information contained in correspondence.

18. Artificial intelligence - permitted assistance

CCC members may use AI to assist with research, drafting, reviewing, summarising, organising, improving wording, spelling and presentation, explaining complex information, generating ideas, and preparing initial policies, reports, briefings and public communications. Using AI for these purposes is not in itself a breach of this policy.

AI is an assistance tool. Protected personal or confidential information should not be unnecessarily disclosed to an AI service, important material must be appropriately checked, and final responsibility for documents and decisions remains with CCC. Where appropriate, CCC may record that AI assistance was used.

19. Information that should not normally be put into public AI systems

Unless there is an appropriate reason and suitable safeguards, members should not enter confidential correspondence, unpublished identifiable complaints, private contact details, health information, financial or banking information, passwords, security information, confidential legal advice, highly sensitive personal information or documents containing unnecessary identifiable personal information into a public generative AI service.

Where an AI, cloud, survey, email or other digital service processes personal information on CCC's behalf, CCC should consider whether the provider is acting as a processor or other third party, what contractual/data-protection terms apply, where data may be stored or transferred, and whether the use is consistent with CCC's Privacy Notice and Register of Processing Activities. The fact that a service is convenient or widely used does not remove these checks.

20. Anonymising information for AI

Where AI could legitimately help with a CCC matter, identifying information should be removed wherever reasonably possible. Names, addresses, telephone numbers, email addresses and other unnecessary identifiers should normally be removed before information is entered into AI.

For example, use 'A resident has complained that...' rather than identifying the resident when their identity is unnecessary to the task.

21. Checking AI output

AI can produce inaccurate, incomplete, misleading, outdated or fabricated information. Important AI-generated information must therefore be appropriately checked.

Particular care should be taken with legal statements, legislation, quotations, statistics, references, allegations, dates and statements attributed to public bodies. AI output should not be treated as authoritative simply because it appears confident or detailed.

22. AI and CCC decisions

AI may assist members in understanding information, but it must not be the sole decision-maker for CCC. AI should not determine whether a complainant is truthful, whether a councillor committed misconduct, whether an allegation is established, whether an individual is credible, or the outcome of a formal CCC decision.

Those judgements remain with the appropriate human decision-makers.

23. Using AI when a member is unsure

CCC members may use AI to help interpret this policy, identify possible GREEN, AMBER or RED issues, and locate questions or authoritative guidance that should be checked.

- Anonymise personal information first wherever reasonably possible.
- Ask AI to identify risks, questions to consider, or authoritative guidance that should be checked.
- Check important advice against the original policy, legislation, ICO guidance or other authoritative source.
- If the matter remains uncertain, potentially serious, or falls within the RED category, seek appropriate human advice before acting.

© Coll Community Council 2026

23A. Using public information with AI

CCC members may use AI to research, analyse, compare, summarise and prepare CCC documents from information legitimately available to the public, including information published on official websites.

This will normally be a GREEN use where the material is genuinely public, the use is legitimate CCC business and unnecessary personal or sensitive information is not being processed.

- Examples include published council policies and reports, Scottish Government material, public consultations, public transport information, published funding information, official statistics and other legitimately public material.
- The fact that information is publicly accessible does not automatically justify reusing every item of personal information for an unrelated purpose.
- Use only the information reasonably necessary for the CCC task.
- Avoid copying unnecessary names, contact details or sensitive personal information into an AI service merely because they appear online.
- Respect copyright and source restrictions where relevant.
- Check important AI-generated facts, quotations, legal statements, dates and references against the original source before CCC relies upon or formally issues the document.
- Where useful, retain or identify the original sources so members and readers can see the basis of significant factual statements.

24. Electronic records and retention

CCC should not retain personal information indefinitely merely because electronic storage is available. Information should be periodically reviewed and information no longer required for a legitimate administrative, governance, historical or legal purpose should be appropriately deleted or destroyed.

Retention should follow CCC's current Register of Processing Activities/retention schedule. At the date of this revised draft, that register specifies: signed minutes - in perpetuity; agendas - 5 years; general correspondence - 3 years; comments and enquiries - 3 years; complaints - 5 years; annual accounts - 6 years from the end of the financial year; surveys - for as long as required for the stated purpose; and meeting recordings used for minute-taking - until the minutes have been written and approved. Where the register is amended, the current approved register takes precedence over this summary.

Official minutes and other records CCC is required or reasonably expected to retain should be preserved appropriately.

25. Data breaches

A possible personal-data breach may include sending information to the wrong person, accidentally publishing personal information, losing a device containing CCC information, unauthorised account access, accidentally sharing a confidential document, inappropriate disclosure through messaging/social media, or entering protected personal information into an inappropriate AI service.

A suspected personal-data breach should be reported internally immediately so that CCC can assess it without delay. If the breach is likely to result in a risk to people's rights and freedoms, the ICO must be notified without undue delay and, where feasible, within 72 hours of CCC becoming aware of it. If the risk is high, affected people may also need to be informed without undue delay. CCC should keep a record of the incident and the assessment, including where a decision is made that ICO notification is not required.

26. Honest mistakes and proportionality

An honest mistake does not automatically amount to misconduct. CCC recognises a difference between an inadvertent mistake, minor procedural error, genuine misunderstanding or promptly corrected error, and reckless handling, knowingly ignoring clear advice, repeated inappropriate conduct, deliberate disclosure of confidential information or intentional misuse of personal data.

Any alleged policy breach should be considered fairly and proportionately, including what information was involved; whether anyone was identifiable; whether information was already legitimately public; sensitivity; purpose; whether it related to legitimate CCC duties; recipients and extent of distribution; whether the member reasonably believed the action appropriate; whether conduct was deliberate, reckless or accidental; whether harm or significant risk resulted; corrective action; and whether clear previous advice had been given.

© Coll Community Council 2026

A policy breach should not be established merely because, with hindsight, another method might have been preferable. This does not override applicable data-protection legislation or other legal obligations.

27. Formal CCC business and decision-making

WhatsApp, Facebook, Instagram, email and AI should not become substitutes for proper CCC governance. Where a matter requires a formal CCC decision, it should be dealt with through the appropriate CCC procedure and properly recorded.

Digital communication may assist preparation, but should not circumvent requirements concerning meetings, minutes, transparency or decision-making. This also supports the 2026 Argyll and Bute framework, which requires community councils to adhere to the law, the Scheme and the Community Councillors' Code of Conduct, and expects decisions/actions to be properly recorded.

28. Subcommittees and working groups

This policy applies, where appropriate, to all official CCC subcommittees and working groups.

29. Responsibility, awareness and review

Every CCC member has responsibility for exercising reasonable care when handling information in connection with CCC duties. CCC should ensure that new members receive this policy, the Quick Guide and relevant data-protection information.

This policy should be read alongside CCC's current Privacy Notice and Register of Processing Activities/retention schedule. The three documents should be reviewed together where a material change is made to CCC's processing purposes, lawful bases, retention periods, digital services or AI use, so that they remain consistent.

This policy should be reviewed at least annually and sooner following significant changes to UK data-protection legislation, ICO guidance, Argyll and Bute Community Council guidance, CCC working practices, digital communication technology, AI technology or experience showing that clarification is needed.

30. Status of external guidance

This policy must not be described as 'ICO approved' unless the ICO has expressly provided such approval.

31. Sources and guidance

The following sources were checked for this final draft. They inform the policy; once adopted, the policy remains CCC's own policy.

- UK GDPR and the Data Protection Act 2018, as amended, including changes introduced by the Data (Use and Access) Act 2025 where applicable.
- Information Commissioner's Office (ICO) - A guide to the data protection principles.
- ICO - A guide to lawful basis; special-category data guidance; data minimisation; accountability and governance; data security; and personal-data breach guidance.
- ICO - Public task guidance (updated 28 August 2026).
- ICO - Artificial intelligence and data protection guidance, including accountability/governance, security, data minimisation, accuracy and AI risk guidance.
- Argyll and Bute Council - Scheme for the Establishment of Community Councils in Argyll and Bute 2026.
- Argyll and Bute Council - Approved Best Practice Agreement 2026.
- Argyll and Bute Council - Community Councils: Data Protection Information.
- Argyll and Bute Council - ICT Acceptable Use Policy and related revision material, considered as useful good-practice reference material only; this policy does not treat that corporate AUP as automatically binding on CCC.
- CCC Privacy Notice 2025 and CCC Register of Processing Activities and retention schedule, used to align internal data-protection arrangements with this policy. *These are CCC internal governance documents and should be kept with the adopted policy set.*

32. Copyright, permitted use and drafting assistance

Copyright and permitted use

© Coll Community Council 2026

© Coll Community Council 2026. This document may be reproduced for non-commercial community-council purposes, provided that Coll Community Council is acknowledged and the content is not presented as having been formally adopted by another organisation.

Drafting assistance

Artificial intelligence tools assisted with drafting, reviewing and formatting this policy. The content was checked and amended by Coll Community Council. Following formal adoption, Coll Community Council accepts responsibility for the final document.

FORMAL ADOPTION

This Digital Communications, Social Media, Data Protection and Artificial Intelligence Policy was considered and formally adopted by Coll Community Council.

Date adopted	
CCC minute reference	
Convenor	
Secretary	
Policy version	1.4
Effective from	
Next review	

MEMBER'S POCKET GUIDE - KEEP THIS PAGE HANDY

For ordinary CCC work, start here. Use the full policy when the issue is more complex.

GREEN

Public and routine information - Normally proceed.

AMBER

Personal or private information - Stop and think. Remove unnecessary personal information. Ask if uncertain.

RED

Sensitive or confidential information - Stop and seek advice.

AI CAN ASSIST - HUMANS REMAIN RESPONSIBLE

© Coll Community Council 2026