Email address and content policy

Last review date	Quarter 3, 2024
Scheduled review date	Quarter 3, 2026
Introduction	The Centre for Community-Driven Research (CCDR) is committed to maintaining the privacy and confidentiality of all stakeholders. Email poses a significant risk in breaching local privacy laws and this policy aims to mitigate those risks.
Lawfulness, fairness and transparency	CCDR must process personal data lawfully, fairly and in a transparent manner in relation to the policy subject.
Purpose limitation(s)	The purpose of this policy is to guide staff in the use of emails addressed to multiple recipients. Where emails are sent to more than one person within the same organisation, this policy does not apply.
Purpose	Email is a tool used primarily for external correspondence at CCDR. Email addresses are identifiable personal data under General Data Protection Regulations (GDPR), so it is important to consider how you include addresses in emails.
Policy	Where emails are sent to more than one direct recipient across a number or organisations or companies, recipient addresses must be entered into the BCC field. Other guidance to maintain privacy are: ▪ Before sending emails, take a minute to double-check that the recipients' emails are correct and, for common names, that it's the right individual - Once the email is sent, it's not possible to retrieve. ▪ Only send emails to those who really need it and be careful when using 'reply to all' - does everyone need to receive your response? ▪ Take care when writing emails – the contents may be used/requested by the individual concerned or read by others. ▪ Make it clear to the recipient if an email is confidential or should not be forwarded to others by writing PRIVATE AND CONFIDENTIAL at the top of the email. ▪ Think carefully when titling emails – make it appropriate to the contents of the email, but do not include personal data ▪ Make sure any attachments which contain information that has been redacted has been done in a permanent way which cannot be reversed by the recipient, meaning they can access the hidden information. - Text which has been highlighted black in a word document in black and converting into PDF is easily reversed. ▪ Always password protect attachments containing highly sensitive information ▪ Do not save emails containing personal data once the information has been stored in a more appropriate place
Policy Implementation and assignment of responsibility	Email addresses are identifiable personal data under GDPR, so it is important to consider how you include addresses in emails. If you do inadvertently send an email containing personal data to an incorrect address or find information has been inappropriately shared/disclosed, please contact the Chief Executive immediately for assistance on the next steps to take.
Related standard operating procedures	Not applicable.