HAWKE'S BAY
REGIONAL COUNCIL

Code of Conduct

2025

Adopted by resolution 12 November 2025

Contents

Part 1 Preliminary

Introduction

1. Clause 15, Schedule 7 of the Local Government Act 2002 provides that the Secretary for Local Government may approve and issue a Code of conduct to apply to members of local authorities, local boards and community boards. Clause 15(4) provides that's members must comply with the Code of conduct.
2. The Code of conduct must set out:
   (a) understandings and expectations adopted by the local authority about the manner in which members may conduct themselves while acting in their capacity as members, including—
      (i) behaviour toward one another, staff, and the public; and
      (ii) disclosure of information, including (but not limited to) the provision of any document, to elected members that—
         (A) is received by, or is in the possession of, an elected member in his or her capacity as an elected member; and
         (B) relates to the ability of the local authority to give effect to any provision of this Act; and
   (b) a general explanation of—
      (i) the *Local Government Official Information and Meetings Act 1987*; and
      (ii) any other enactment or rule of law applicable to members.
3. This document sets out the Code of conduct provided for in Clause 15, Schedule 7 of the Act.

Application

4. This Code applies to:
   - Members of the governing body of a local authority
   - Members of a local board
   - Members of a community board
   - Members of a committee or sub-committee appointed under clause 31(3), Schedule 7 of the Local Government Act 2002 or pursuant to another Act, while acting in their capacity as a member of a local authority, local board, community board, committee or sub-committee.

Interpretation

5. In this Code:

   Complainant means a person who has made a complaint

   Council group means a local authority and its related local boards, community board, committees and sub-committees

   Investigator means a person appointed to investigate and determine a complaint appointed from outside the membership and employees of a local authority

   Member means a member of a local authority, local board, committee or subcommittee, and includes a Mayor or a Chairperson

   Respondent means a member who is the subject of a complaint

Part 2 Expectations and behaviours of members

General expectations of members

1. The Chairperson of Hawke's Bay Regional Council is expected to take a lead in developing and maintaining a constructive culture amongst the members of the Council.
2. Members are expected to:
    2.1. contribute to developing and maintaining a constructive culture amongst the members of the Council, committee or sub-committee of which they are a member
    2.2. use their best endeavours to resolve issues outside of the Code of Conduct complaints process
    2.3. attend any induction programmes organised by HBRC for the purpose of facilitating agreement on Council's vision, goals and objectives and the manner and operating style by which members will work
    2.4. take part in any assessment or evaluation of Council's performance and operating style
    2.5. take all reasonable steps to acquire and maintain the required skills and knowledge to effectively fulfil their declaration of office and contribute to the good governance of the Hawke's Bay Regional Council.

Te Tiriti o Waitangi

3. Members are expected to operate and make decisions in manner that recognises and respects the significance of Te Tiriti o Waitangi taking into account the following principles[1]:
    3.1. Tino Rangatiratanga: The principle of self-determination provides for Māori self-determination and mana motuhake. This requires local authorities to be open to working with mana whenua partners in the design and delivery of their work programmes,
    3.2. Partnership: The principle of partnership implies that local authorities will seek to establish a strong and enduring relationship with iwi and Māori, within the context of iwi and Māori expectations. Kaunihera should identify opportunities, and develop and maintain ways for Māori to contribute to kaunihera decisions, and consider ways kaunihera can help build Māori capacity to contribute to council decision-making,
    3.3. Equity: The principle of equity requires local authorities to commit to achieving the equitable delivery of local public services,
    3.4. Active protection: The principle of active protection requires local authorities to be well informed on the wellbeing of iwi, hapū and whanau within their respective rohe,
    3.5. Options: The principle of options requires local authorities to ensure that its services are provided in a culturally appropriate way that recognises and supports the expression of te ao Māori.

Behaviours

4. Clauses 10 to 12 of this Code set out understanding and expectations about the manner in which members should conduct themselves while acting in their capacity as members.

Trust

5. Members will:
    5.1. make decisions on their merits, in the interests of the public and unaffected by illegitimate considerations such as personal interest or other duties or relationships
    5.2. disclose personal and outside interests, relationships and duties

[1] Sourced from the LGNZ Code of Conduct template 2022.

5.3. declare a conflict of interest and step aside from a decision where they are unable to approach a decision on its merits or it might appear that they will not approach a decision on its merits, in the interests of the public and unaffected by a personal or outside interest, relationship or duty

5.4. when making decisions, have an open mind to the views of others and to alternatives, and be prepared, despite any predisposition they may have, to change their mind

5.5. ensure that they are not under an obligation to those who might inappropriately try to influence them in the performance of their duties

5.6. be accountable for the decisions they make and enable appropriate public scrutiny

5.7. make an equitable contribution, including attending meetings and workshops, preparing for meetings, attending civic events, and participating in relevant training seminars

5.8. act and make decisions openly and transparently

5.9. be truthful and demonstrate honesty and integrity

5.10. use council resources prudently and lawfully and not for their own purposes

5.11. uphold the law, and promote and support high standards of conduct by leadership and example

5.12. comply with the policies and protocols adopted with this Code.

Respect

6. Members will:

6.1. respect the people they work with

6.2. interact with other elected members, staff and the public in a way that:

6.2.1. encourages mutual respect and maintains the dignity of each individual o recognises others' roles and responsibilities

6.2.2. is inclusive

6.2.3. enables the co-existence of individual and collective responsibility

6.2.4. allows for robust discussion and debate focusing on issues rather than personalities

6.2.5. is not derogatory

6.2.6. encourages thoughtful analysis

6.2.7. maintains public confidence in the office to which they have been elected

6.2.8. is open and honest

6.2.9. maintains the confidentiality of confidential information provided to them.

Policies

7. Members are expected to be aware of and comply with the following policies of the local authority:

7.1. Conflicts of interest (Appendix 1)

7.2. Protected Disclosures Policy (Appendix 2)

7.3. Privacy Policy (Appendix 3)

7.4. Gifts, Hospitality and Winnings Policy (Appendix 4)

7.5. Media Policy (Appendix 5)

7.6. Social Media Policy (Appendix 6)

7.7. Risk Management Policy (Appendix 7)

7.8. HBRC Generative AI Policy (Appendix 8)

7.9. ICT Acceptable Use Policy (Appendix 9)

Part 3 Breaches and complaints

Breaches of the Code

8. A breach of this Code occurs if:
    8.1. One or more of the principles listed in paragraphs 10 to 11 are breached
    8.2. A policy listed in paragraph 7 is breached.

Complaints

Who may make a complaint?

9. Complaints about an alleged breach of this Code by a member may be made by:
    9.1. Members of the Council, committee or sub-committee
    9.2. An employee of HBRC
    9.3. A member of the Public.

Making a complaint

10. Where a person listed in paragraph 14 believes that a member has breached this Code that person may make a complaint.
11. A complaint must be made in writing and lodged with the Chief Executive, and:
    11.1. Describe the breach
    11.2. Reference the part of this Code which is alleged to have been breached
    11.3. Provide evidence of the alleged breach, and
    11.4. Provide evidence of any attempts to resolve the breach prior to the complaint having been lodged.

Member's capacity

12. A complaint must relate to the conduct of a member while acting in their capacity as a member.
13. For the avoidance of doubt, this Code applies to any interaction between a member and an employee of the Council where:
    13.1. The member is acting in a personal capacity; and
    13.2. The employee is employed by the local authority forming part of the council grouping the member relates to.

Principles and materiality

Principles for dealing with complaints

14. Complaints will be considered and dealt with in accordance with the following principles:
    14.1. The approach for investigating and assessing a complaint will be proportionate to the apparent seriousness, nature and complexity of the alleged breach.
    14.2. The concepts of natural justice, fairness and reasonableness will apply in the determination of any complaints made under this Code.

Information privacy principles

15. When receiving or collecting information about a complaint or when providing information about a complaint the Chief Executive and the investigator shall apply the information privacy principles set out in section 22 of the Privacy Act 2020.

Materiality

16. An alleged breach under this Code is material if, in the opinion of an investigator, it would if proven, bring a member or the local authority into disrepute or, if not addressed, reflect adversely on another member of the Council.

17. The following may be taken into account when assessing materiality:

    17.1. The conduct was not stopped on request

    17.2. The conduct appeared to be intentional, malicious or motivated by ill-will

    17.3. The conduct caused serious harm, such as reputational harm for an individual or organisation, bringing the local authority into disrepute

    17.4. There has been an ongoing pattern of breaches

    17.5. Even though the conduct complained of occurs on only one or two occasions it represents a major departure from expected standards.

18. The following types of conduct shall be dealt with by an investigator as if they were material:

    18.1. participating in a decision where the member has been formally advised through the 'conflict of interest' provisions Part 4 of this Code that a conflict of interest exists

    18.2. bullying, aggressive or offensive behaviour

    18.3. discrimination

    18.4. undermining the role of other elected members

    18.5. misrepresentation of the statements or actions of others

    18.6. disclosure of confidential information

    18.7. misuse of council resources

    18.8. harassment, including

        18.8.1. violent threats or language directed against another person

        18.8.2. discriminatory jokes and language o posting sexually explicit or violent material

        18.8.3. posting (or threatening to post) other people's personally identifying information

        18.8.4. personal insults

        18.8.5. unwelcome sexual attention

        18.8.6. advocating for, or encouraging, any of the above behaviour.

    18.9. publicly criticising staff or calling into question their professionalism or integrity.

Process for dealing with complaints

Chief Executive receives complaint

19. On receipt of a complaint under this Code the Chief Executive will refer the complaint to an investigator. The Chief Executive will also:

    19.1. inform the complainant that the complaint has been referred to the investigator and the name of the investigator, and refer them to the process for dealing with complaints as set out in this Code

    19.2. inform the respondent that a complaint has been made against them, the name of the investigator and remind them of the process for dealing with complaints as set out in this Code.

Investigator makes preliminary assessment

20. On receipt of a complaint the investigator will undertake a preliminary assessment to determine the relative merit and seriousness of the alleged breach and the nature of the subsequent process that will be followed. The investigator will consider whether:

    20.1. the complaint is trivial, vexatious, frivolous, not made in good faith or politically motivated and should be dismissed

    20.2. the complaint is without substance, or does not appear to be a breach of this Code and should be dismissed

    20.3. the complaint is relatively minor and no further action is necessary

    20.4. the complaint is outside the scope of this Code and should be re-directed to another agency or process

    20.5. The complaint is not material and should be referred to the Chairperson to be dealt with under paragraph 33

    20.6. The complaint should in the first instance be dealt with by mediation

    20.7. the complaint is material and a full investigation is required.

21. Factors that can be considered when determining if a complaint is trivial, frivolous, vexatious, not made in good faith, or without substance include whether complaints are intended to:

    21.1. intimidate or harass another member or employee

    21.2. damage another member's reputation

    21.3. obtain a political advantage

    21.4. influence the Council in the exercise of its functions or to prevent or disrupt the exercise of those functions

    21.5. avoid disciplinary action under this Code

    21.6. prevent or disrupt the effective administration of this Code.

22. In making the assessment the investigator may make whatever initial inquiry is necessary to determine their recommendations, including interviewing relevant parties.

23. Subject to clause 29, a full copy of the complaint will be provided to the respondent which will include the name of the complainant.

24. Where appropriate and having considered relevant matters such as natural justice obligations, legal issues, privacy issues and potential prejudice to the future supply of complaint information the investigator may:

    24.1. Decline to provide a copy of the complaint to the respondent, or

    24.2. Provide a redacted copy of the complaint to the respondent.

Outcomes of preliminary assessment

25. Where an investigator determines that a complaint is trivial, vexatious, frivolous, or politically motivated, the complaint may be dismissed. The Chief Executive will advise both the complainant and the respondent of the investigator's decision.

26. Where the investigator finds that the complaint involves a potential legislative breach and/or is outside the scope of this Code, they may recommend that it should be re-directed by the Chief Executive to another agency or process. The Chief Executive will advise both the complainant and the respondent of the investigator's decision.

27. If the complaint is not dismissed or redirected, the investigator may initiate any of the following processes:

    27.1. referral to the Chairperson

    27.2. mediation

    27.3. a full investigation.

Referral to Chairperson

28. If the subject of a complaint is found to be non-material (not serious) and not amenable to mediation, the investigator will inform the Chief Executive and suggest that the respondent is referred to the Chairperson for advice and guidance. A meeting or meetings with the Chairperson will be regarded as sufficient to resolve the complaint. The investigator may also recommend a course of action appropriate to the breach for the Chairperson 's consideration, such as:

    28.1. that the respondent attend appropriate courses or programmes to increase their knowledge and understanding of the matters resulting in the complaint

    28.2. that the respondent work with a mentor for a period

    28.3. that the respondent tenders an apology to the complainant.

29. The Chief Executive will advise both the complainant and the respondent of the investigator's decision and any recommendations, neither of which are open to challenge.

30. The outcomes of any referral to the Chairperson will be confidential and, other than reporting that a complaint has been resolved through referral to the Chairperson for guidance, there will be no additional report to Council.

Mediation

31. If the complaint concerns a dispute between two members, or between a member and another party, the investigator may recommend mediation.

32. The investigator will contact the parties and seek their agreement to independently facilitated mediation.

33. If the parties agree and the issue is resolved by mediation the matter will be closed and no further action is required. The outcomes of any mediation will be confidential and, other than reporting that a complaint has been resolved through mediation, there will be no additional report to council unless the complaint is referred for further investigation due to a failure of the mediation process.

34. The investigator will use their best endeavours to resolve a complaint through mediation before determining that a complaint is to be resolved through an investigation.

Referral for full investigation by investigator

35. If the subject of a complaint is found by the investigator to be material or if no resolution can be reached through mediation and/or mediation is refused by the complainant or the respondent, the investigator will inform the Chief Executive that the matter should proceed to full investigation and the Chief Executive will inform the complainant and respondent.

Investigator to undertake full investigation

36. Where a complaint proceeds to full investigation the investigator will undertake an investigation appropriate to the scale of the seriousness of the alleged breach and in doing that may:

    36.1. consult with the complainant, respondent, and any directly affected parties

    36.2. undertake a hearing with relevant parties

    36.3. refer to any relevant documents or information.

37. Following an investigation the investigator may uphold the complaint in whole or in part, or dismiss the complaint.

38. Where a complaint is upheld, the investigator will also determine whether to impose any of the following sanctions[2] on the member:

    38.1. a requirement to apologise and, if applicable, withdraw remarks

    38.2. a requirement to make a public statement correcting or clarifying previous remarks

    38.3. a requirement to undertake specified training or personal development

    38.4. suspending the elected member from committees or other representative bodies

    38.5. requiring the member to seek guidance from the chairperson or a mentor

    38.6. for a nominated period, restrict the member's access to Council staff (other than the Chief Executive or their specific nominees) and/or to Council offices or parts of Council offices.

39. In deciding whether to impose a sanction, and what the sanction should be the investigator must take into account the materiality of the breach.

40. Following the investigation, the investigator will provide the Chief Executive with a report on the findings of the investigation and any sanctions that are imposed on the respondent.

41. The Chief Executive will within 2 weeks of having received it provide the report to the complainant, respondent, and the relevant local board or governing body for information purposes only.

42. There is no right of appeal of any decision made by the investigator.

Public disclosure of complaints and outcomes

43. The public interest in the accountability of elected members needs to be balanced against the requirements of natural justice and privacy. The outcomes of complaints relating to non-material breaches will not be publicly reported by the Council, except in an anonymised form for the purpose of sharing good practice.

44. Where the complaint relates to a material breach of this Code, the investigator will determine whether the outcome of the investigation, or the report, should be publicly reported (having regard to Local Government Official Information and Meetings Act 1987). If such information is publicly reported, compliance with any sanctions imposed by the investigator will also be publicly reported.

[2] The terms of reference given by the Minister of Local Government exclude from the Commission's consideration (1) disqualification from office as a potential penalty; (2) creation of offences. These issues, along with the wider issue of sanctions, are being considered by the Department of Internal Affairs and the Department's work may result in proposals to amend the legislation in relation to disqualification and offences. This part of the draft Code may require change after the outcome of the Department's work is known.

After a complaint has been dealt with

45. After a complaint has been dealt with:

    45.1. Members should reflect on how to rebuild any relationships impacted by the cause of a complaint.

46. The Chief Executive shall consider whether there are administrative actions that can be taken to help ensure that the causes of a complaint are less likely to occur in the future or that the negative impacts of those causes can be better mitigated.

Part 4 Conflicts of interest

47. Members are expected to:

    47.1. Maintain a clear separation between their personal interests and their duties as members in order to ensure they are free from bias or predetermination (either real or perceived) when making decisions

    47.2. Familiarise themselves with the provisions of the Local Authorities (Members' Interests) Act 1968 in relation to pecuniary interests

    47.3. Familiarise themselves with the policies and protocols of the local authority relating to conflicts of interest

    47.4. Identify actual or perceived conflicts of interest existing in relation to a matter they may make decisions on, and taking appropriate action to ensure they do not compromise the decisions of the local authority, board or committee they are a member of

    47.5. Seek advice from the Chief Executive or other appropriate officer of the Council about conflict of interest issues.

48. Where an alleged breach of this Code relates to a conflict of interest, the Chief Executive will inform the respondent of the complaint and arrange for the member to receive advice from the Chief Executive on the conflict of interest.

49. The Chief Executive will inform the complainant that advice on the matter has been sought. The complainant will not have any further involvement in the complaint following this.

50. The advice is provided to the member and to the Council (in relation to a complaint against a Council member).

51. If the advice is that it would be reasonable to conclude that the member has a conflict of interest, they are required to declare the conflict and recuse themselves from any future decision on that matter to which the conflict of interest relates and while the interest continues to exist. If the elected member does not take that action, the matter will be referred to an Investigator who will consider whether it should be investigated as a material breach of this Code.

Part 5 Rights and obligations of members

52. This Part of the Code provides an outline:

    52.1. of members' rights and obligations

    52.2. the ability of members to access information as part of their role.

Obligations of members

53. The obligations of members include:

    53.1. Taking responsibility for ensuring they understand their roles and responsibilities and this Code, and attending any appropriate training opportunities provided by the local authority

    53.2. Attending all meetings (including external organisations to which they are appointed), workshops and working groups

    53.3. Coming to meetings prepared, including having read relevant material

    53.4. Seeking personal and skill development opportunities to effectively fulfil their statutory declaration of office and contributing to the good governance of the local authority

    53.5. Ensuring that pecuniary interest returns are provided in an accurate and timely manner.

Rights of members

54. The rights of members include:

    54.1. subject to any conflicts of interest identified:

        54.1.1. the right to attend and participate in any meeting of the local authority, local board, community board, committee or subcommittee they are a member of

        54.1.2. the right to vote on decisions to be made by the local authority, local board, community board, committee or sub-committee

    54.2. the same rights as members of the public to request information under the Local Government Official Information and Meetings Act 1987.

    54.3. the right, under section 26A of the Local Government Act 2002 to access information held by the Council.[3]

Access to information

55. Section 26A of the Local Government Act 2002 sets out the entitlement of members access to documents held by Council. These are that:

    55.1. A member of a local authority is entitled to have access to documents held by the local authority that are reasonably necessary to enable the member to effectively perform their duties as a member of the local authority.

    55.2. A member of a local authority may request access to the documents specified in subclause (61.1) from the Chief Executive of the local authority.

[3] The ability for members to access information under section 26A is proposed to be included in the Local Government Act 2002 by the Local Government (System Improvements) Amendment Bill.

Part 6 Freedom of expression

56. This Part of the Code provides an explanation of how freedom of expression as guaranteed by the New Zealand Bill of Rights Act 1990 applies, including the limits placed on this right by other statutes such as the incitement provisions of the Human Rights Act 1993.

57. Section 14 of the New Zealand Bill of Rights Act 1990 provides that:

    57.1. Everyone has the right to freedom of expression, including the freedom to seek, receive, and impart information and opinions of any kind in any form.

58. The Code of conduct is not a means of preventing members from expressing their personal views provided they are clearly signalled as personal views. Rather the Code is designed to permit robust debate and the expression of a variety of points of view by providing a framework to ensure that debate is conducted in a civil and respectful way.

59. The right to freedom of expression should be used responsibly and not be used to breach the Code in a manner that is, for example, disruptive or derogatory.

60. Somes Acts contain specific limitations to the freedom of expression. These include limitations relating to:

    60.1. Discrimination causing racial disharmony, section 61, Human Rights Act 1993

    60.2. Communication constituting sexual harassment, section 62. Human Rights Act 1993

    60.3. Communication constituting racial harassment, section 63, Human Rights Act 1993

    60.4. Communication Inciting racial disharmony, section 131, Human Rights Act 1993

    60.5. Offensive behaviour or language, section 4, Summary Offences Act 1981

    60.6. Posting a digital communication with the intention it causes harm to a victim, section 22, Harmful Digital Communications Act 2015

    60.7. Privacy breaches under the Privacy Act 2020, including those causing interference with the privacy of an individual, as described in section 69 or breaches that either have caused or are likely to cause anyone serious harm as described in section 112

    60.8. In relation to offers of stocks or bonds, disclosure of information that breaches the Financial Markets Conduct Act 2013, in particular Part 2 relating to fair dealing, Subpart 2 of Part 5 relating to insider trading, and Subpart 3 of Part 5 relating to market manipulation

    60.9. The Defamation Act 1992, which gives individuals the right to seek remedy against false statements that could harm reputation.

Part 7 Selecting the initial assessor and independent investigator

Selecting an initial assessor

61. The chief executive is responsible for this. In selected the initial assessor, the chief executive will consult with the local authority.

62. The initial assessor should be a person, or a position, that is independent of a local authority's political governance, while also being easily accessible, as their role is crucial if complaints are to be expedited quickly and without controversy. For example:

    62.1. The external appointee on a kaunihera's Audit and Risk Committee

    62.2. A member of staff, such as an internal ombudsman or ethics adviser, as long as they have operational independence from the chief executive (similar to the independence afforded an Electoral Officer).

    62.3. A retired local authority chief executive.

    62.4. A retired local authority politician

    62.5. A member of the public with relevant experience and competency.

Selecting an independent investigator4

63. The chief executive is responsible for compiling a panel or list of independent investigators.

64. At the beginning of each triennium the chief executive, in consultation with the kaunihera, will compile a list of independent investigators. In selecting them, a chief executive may consider:

    64.1. the council's legal advisers,

    64.2. a national service specialising in public sector integrity,

    64.3. a national service providing assessment and investigation services, or

    64.4. an individual with relevant skills and competencies.

Please note: Given the litigious nature of some code of conduct disputes independent investigators should have relevant liability insurance, provided on their own behalf or by the local authority. The Chief Executive also needs to ensure that investigations are undertaken within budgetary limits negotiated in advance.

4 At time of publication LGNZ is exploring options for the establishment of a national investigation and assessment service.

Policy

Title:	Conflicts of Interest Policy
Policy number:	CD0004

Team policy owned by:	Risk and Assurance	**Version number:**	2
Document owner:	Helen Marsden	**Date policy last reviewed and published:**	2024/12/17
Document approver:	Susie Young	**Next review due:**	2026/12/17

Purpose

It is important that public and key stakeholders have trust and confidence in Hawkes Bay Regional Council (HBRC). Therefore, HBRC must retain the ability to be, and be seen as, impartial in all-decision making. This means elected members, Sub-committee appointees, employees, contractors and casuals to HBRC need to use sound judgement by declaring and managing any potential conflict of interest. This policy sets out the requirements for identifying and managing both perceived and actual conflicts of interest.

Target audience

This policy applies to all HBRC elected members, sub-committee appointees, staff, and contractors of HBRC.

All elected members and Sub-Committee appointees before applying this policy must in the first instance meet their obligations as detailed in the Local Authorities (Members' Interests) Act 1968.

Policy details

1. **Policy goal or objective**

   1.1. The goal of this policy is to ensure that all potential or actual conflicts are raised by HBRC's interested parties as soon as practical. This enables HBRC to proactively manage the potential or actual conflict to retain public and key stakeholder confidence in HBRC.

2. **Related documents (e.g., Legislation, Policies, SOPs, etc)**

   - Internal Fraud Policy - CD0003
   - Gifts, Hospitality and Winnings Policy - CD0005
   - Procurement Policy - CD0007

3. **Key definitions/abbreviations**

   3.1. **Close connection** – includes any immediate family member, any business relationship, close personal relationship, or active membership of a group/society of HBRC's interested party.

   3.2. **Conflict of interest** – a situation where duties or responsibilities of an interested party of HBRC conflict, or could be seen to conflict, with some other interest you might have outside of work.

3.3. **Interested Party** - means elected members, Sub-committee appointees, employees, and contractors of HBRC.

4. What is a conflict of interest?

4.1. A conflict of interest is any situation where the independence, objectivity, or impartiality of an 'interested party' being an elected member, sub-committee appointee, employee, or contractor of HBRC's could potentially be doubted or challenged. A conflict of interest can happen when official duties and personal interests or responsibilities overlap. Conflicts of interest can be financial, non-financial or both.

4.2. A conflict of interest can be:

- **Actual:** where a conflict currently exists between official duties and personal interests' responsibilities.
- **Potential:** where a conflict could happen or is about to happen, or
- **Perceived:** a situation where other people might reasonably think a conflict exists

4.3. It is important to understand that the existence of a conflict of interest does not necessarily imply wrongdoing on the part of any person. However, any interest which either does, or could, give rise to a conflict of interest must be disclosed to HBRC.

5. Why register an interest?

5.1. The main goal of managing conflicts of interest is to ensure that decisions are made – and are seen to be made – on proper grounds, for legitimate reasons and without bias.

5.2. Therefore, it is expected that any actual, potential, or perceived conflict of interest is declared. If in doubt whether the interest is a conflict you should err on the side of caution and declare the interest. Proactively disclosing an interest in HBRC's confidential interest register located on Kowharawhara under 'I want to …' provides the greatest protection from non-compliance with this policy. Section 11 of this policy outlines who is notified of interests as they are declared.

6. Examples of potential conflicts of interests:

6.1. Potential conflicts of interests can arise in several ways. The following list, while not exhaustive, provides commonly understood conflicts:

- Procuring products or services from an organisation that the HBRC interested party is invested in.
- Procuring products or services from an organisation where HBRC's interested party has a close connection involved in the organisation.
- HBRC's interested party is involved in the issue, monitoring or enforcement of any consent, compliance or community activity and the applicant or holder is a close connection.
- Being involved in HBRC's selection or interview process where the applicant is a close connection.
- Where the interested party of HBRC is given something (gift, hospitality, or travel etc) from someone who could benefit from their decision.

- Where a supervisor, manager, or anyone with authority over others' terms and conditions of employment is in a romantic or close personal relationship with a subordinate (refer section 8 of this policy).
- Where the interested party holds a strong personal view on the decision being made e.g., political view, religious belief etc.
- Where the interested party could Influence or participate in a decision to award grants or contracts and is a close connection of the person or organisation that submitted an application or tender.
- Where the interested party is investigating a complaint and is close connection to either the complainant or the person or entity being complained about.
- Owning shares in, or working for, an organisation that has dealings with HBRC where HBRC's interested party has direct involvement in decision making involving that organisation.
- Where the interested party is a member of a club, society or association that is directly engaging with HBRC.

7. **Conflicts of interest relating to other employment**

7.1. Other activities or employment, contract, self-employment (paid and unpaid) is permissible. However, to ensure the primary obligation to HBRC is not unduly impacted through an actual or perceived conflict, other activities or employment must be declared. The declaration must include information about the employment/activity and the level of commitment (number of hours).

7.2. If HBRC has genuine reasons based on reasonable grounds for prohibiting or restricting work or activities those reasons will be set out in your employment agreement or relevant employment agreement schedule. Genuine reasons include but are not limited to:

- protecting HBRC's commercially sensitive information
- intellectual property rights
- commercial reputation, or
- any other factors detrimental to HBRC

7.3. Any other employment or activity must not involve the use of HBRC's materials, plant, or information/data without the Group Managers prior written approval.

8. **Conflicts of interest relating to employee personal relationships**

8.1. HBRC does not prevent the development of friendships or romantic relationships between co-workers. However, individuals in roles that are:

- supervisory
- managerial, or
- have authority over others' terms and conditions of employment

Due to their:

- status as role model
- access to personal information, and
- ability to effect employment of individuals in subordinate positions

Must declare any change in relationship status with subordinates through the confidential interest register on Kowharawhara under 'I want to …', or directly to the P&C Manager, without delay.

8.2. When a conflict of interest or potential conflict is identified due to an HBRC employee's relationship with a co-worker, HBRC will work with the parties. HBRC will aim to make sure the parties no longer work together on matters where one is able to influence the other or act for the other. Matters such as hiring, firing, promotions, performance management, compensation decisions and financial transactions are examples of situations that may require relocation of duties to avoid any actual or perceived reward or disadvantage. In some cases, other measures may be necessary, such as transfer of one or both parties to other positions and departments. If one or both parties refuse to accept a reasonable solution, such refusal may be deemed a voluntary resignation.

8.3. Provision of section eight of this policy applies regardless of the sexual orientation of the parties involved.

8.4. In addition, to the interest being declared employees during work time are expected to conduct themselves in an appropriate workplace manner that does not interfere with others or with overall productivity.

8.5. During non-working time, such as lunches, breaks and before and after work periods, employees engaging in personal exchanges in non-work areas should observe an appropriate workplace manner to avoid offending other workers or putting others in an uncomfortable position.

8.6. Employees must not engage in physical contact that would in any way be deemed inappropriate in the workplace by a reasonable person while anywhere on the company premises, whether during working hours or not

9. **How to raise a potential interest?**

9.1. If you believe you have an interest or a potential conflict of interest it is important to declare your interest without delay. An interest is declared through HBRC's confidential interest register located on Kowharawhara under 'I want to …'. If you are an employee or contractor and you do not have access to Kowharawhara then you will need to declare the interest to your Line Manager or overseeing Manager e.g., the Contract Manager. Either your Line Manager or overseeing Manager will then enter your interest declaration into the register on Kowharawhara on your behalf. For Elected Members and Sub-Committee appointees any potential interests that fall outside of the Local Authorities (Members' Interest) Act 1968 will need to be declared to the Strategy and Governance Team who will enter the interest into the register.

9.2. Registering an interest through the interest register in Kowharawhara under 'I want to …' will ensure that the declaration proceeds through an automated workflow to sign-off. Note: Any conflicts that arise through the procurement process must first be advised to the Procurement Team as part of the Procurement Policy and then added as an interest into the interest register on Kowharawhara.

9.3. Once an interest is registered in Kowharawhara under 'I want to …' the system will automatically notify your manager. Your manager in consultation with you as the interested party, will decide what, if any, additional measures are required to manage the potential conflict. The agreed actions must be recorded in the Interest register. It is important to note if no potential conflict is identified 'no action' is required to be taken. Therefore, for audit trail purposes 'no conflict and no action required' must be noted in the register against the declared interest.

9.4. Through the interest register system on Kowharawhara the Line Manager will then submit the declared interest with agreed actions to be taken to the Group Manager, or if you are a Group

Manager to the Chief Executive (CE) for final approval. A notification is also automatically generated and sent to the P&C Manager and the Risk and Corporate Compliance Team Leader.

9.5. When the Group Manager, or in the case of the alternate the CE, receives the declared interest with agreed actions they will either:

9.5.1. Approve the declared interest and agreed actions, or

9.5.2. Reject the declared interest and agreed actions, stating what additional actions need to be taken to manage the conflict.

9.6. When the Group Manager, or in the case of the alternate the CE, has approved the declared interest and agreed actions the system will send a notification, of approval, to the Line Manager and the Interested Party.

9.7. If the Group Manager, or in the case of the alternate the CE, rejects the declared interest and agreed actions the system will send a notification to the Line Manager and Interested Party. The notification will include the additional actions the Group Manager, or in the case of the alternate the CE, requires for the conflict to be adequately managed. The Line Manager and Interested Party then agree these additional actions, update the actions in the register and then resubmit the declared interest and agreed actions to the Group Manager, or in the case of the alternate the CE, for final approval.

9.8. Once the declared interest and agreed actions have had final approval from the Group Manager, or in the case of the alternate the CE, it is the responsibility of the Line Manager to ensure the agreed actions are implemented by the Interested Party.

9.9. For the avoidance of doubt, this policy does not preclude you as an interested party from participating in democratic processes such as submitting on a resource consent or other HBRC proposals that directly affect you. However, you should make it clear that you are making such a submission as a private citizen. It is recommended that staff obtain advice from their manager before making such a submission on whether an interest should be declared.

10. How are actual or perceived interests managed?

10.1. There are a few options for managing actual or perceived interests. Your manager will discuss and agree these with you. The following list, while not exhaustive, provides the more commonly used actions:

- Seeking consent of all affected parties for an exemption so the interested party can be involved
- Imposing additional supervision, oversight, or review over the interested party
- Withdrawing from discussion or decision-making on a particular issue
- Exclusion from a committee or working group dealing with the issue
- Withholding certain confidential information or placing restrictions on access to information
- Negotiating for the transfer of the employee [temporarily or permanently] to another position or project
- Relinquishing the private interest
- Resignation from one or other position or entity

10.2. The assessment to determine which actions to take to address the actual or perceived conflict should consider factors such as:

- The type, size, and level of interest of HBRC's interested party
- The nature or significance of the particular decision or activity being carried out by HBRC
- The extent to which the interested party's other interest(s) could specifically affect, or be affected by HBRC's decision or activity; and
- The nature or extent of the interested party's current or intended involvement in HBRC's decision or activity

10.3. If the interest does not constitute a conflict and therefore does not justify taking any action because it is too indirect or insignificant. Recorded in the in interest register that no conflict was identified so no further action is required.

11. **Roles and responsibilities**

11.1. Interested Party must:

- Declare the interest in accordance with this policy
- Attach any relevant information to the declaration, and
- Undertake all actions agreed to manage the potential conflict of interest.

11.2. Line Manager must:

- Ensure the declared interest is registered in HBRC's interest register through Kowharawhara under 'I want to …'
- Agree appropriate actions with the interested party that must be undertaken to manage any potential conflict of interest
- Attach any further information of relevance to the declaration
- Submit the interest declaration and agreed actions to the Group Manager for review and final approval, and
- Ensure the agreed actions to manage any potential conflict are undertaken by the interested party

11.3. Group Manager, or in the case of the alternate the CE, must:

- Advise, if applicable, through rejecting the declared interest in Kowharawhara any additional or alternative actions to be undertaken by the Interested Party to manage the potential conflict, and then
- Approve through Kowharawhara the declared interest and all agreed actions for managing any potential conflict of interest

11.4. P&C Manager

- Receives notifications of all interests registered through Kowharawhara, and
- Escalates those potential conflicts of interest to the CE, or Council, as deemed appropriate

11.5. Risk and Corporate Compliance Team Leader

- Receives notification of all interests registered through Kowharawhara, and
- From time to time may undertake an audit to ensure that the agreed actions to manage the potential conflicts were complied with

12. **Breach of policy – consequences of non-compliance**

12.1. This policy would be considered breached if you as an interested party do not register a potential conflict of interest. Or, after registering a conflict of interest fail to follow the agreed actions. A breach of this policy may give rise to disciplinary action for serious misconduct.

Summary of key document changes and version control				
Version	**Date**	**Key changes to be communicated to staff**	**Document owner**	**Approver**
1.0	11/10/22	Full redraft with expanded definition to include close personal relationship with subordinates. And the addition of an interest register accessible through Kowharawhara - "I want to…' for staff to declare interests. Supersedes policy SP028 Conflicts of Interest	Risk and Corporate Compliance Manager	Group Manager Corporate Services
2.o	29/10/2024	Annual Review, small grammar and job title changes made.	Risk & Corporate Compliance Team Leader	Group Manager Corporate Services

Policy

Title:	Protected Disclosure Policy
Policy number:	CD0006

Team policy owned by:	People and Capability	**Version number:**	2
Document owner:	Liana Monteith	**Date policy last reviewed and published:**	08/08/2023
Document approver:	Dr Nic Peet	**Next review due:**	08/08/2025

Purpose

The Protected Disclosure Act was originally introduced in 2000 and required Hawke's Bay Regional Council (HBRC) to maintain a staff policy that outlines HBRC's escalation criteria for serious wrongdoing in the workplace. When escalating concerns of serious wrongdoing (sometimes called whistleblowing) staff must reasonably believe it to be true and must follow HBRC's Protected Disclosure Policy.

Target audience

This policy applies to any individual who is (or was formally): an elected member, sub-committee appointee, employee, contractor, or third party in relation to any activity carried, sponsored or supported by HBRC.

Policy details

1. **Policy goal or objective**

   1.1. HBRC's objectives for this policy are to:

   - facilitate the disclosure and investigation of serious wrongdoing in the workplace
   - ensure individuals disclose concerns of serious wrongdoing (see clause 4 of this policy)
   - ensure individuals feel protected when disclosing concerns of serious wrongdoing that they reasonably believe is true or likely to be true, and
   - ensure HBRC are compliant with the Protected Disclosure Act (PDA) 2022

2. **Related documents**

   2.1. Internal Fraud Policy – CD0003

   2.2. Health and Safety Policy – CD0010

3. **Key definitions/abbreviations**

   3.1. **Escalation -** process of bring to the attention concerns/context of the right people (usually management) concerns in order to resolve a challenging situation

3.2. **Internal Fraud -** illegal or unethical activities by an elected member, sub-committee appointees, employee or contractors done in a dishonest, deceptive or unscrupulous manner with the intention of obtaining an advantage, avoiding an obligation or causing loss/harm to another party

3.3. **Investigation -** a thorough search for facts, especially those that are hidden or need to be sorted out. The goal of an investigation is usually to determine how, why or what happened.

3.4. **PDA Coordinator -** HBRC's P&C Manager acts as HBRC's Protected Disclosure Act (PDA) Coordinator

3.5. **Risk –** the effect of uncertainty on objectives

3.6. **Serious wrongdoing –** includes any unlawful activity, gross negligence, criminal offences or conduct that could potentially pose a risk to the public on a broader scale. The Act describes the following as serious wrongdoing:

- unlawful, corrupt or irregular use of public money or resources
- conduct that poses a serious risk to public health, safety and the environment
- conduct that increases the risk of unauthorised intervention from a third-party to encourage a lawsuit
- any kind of criminal offence
- gross mismanagement and negligence from public officials

4. What is 'Serious Wrongdoing'?

4.1. Section 10 of the PDA 2022 defines serious wrongdoing as an act, omission or course of conduct that is:

Type of serious wrongdoing	Does it apply to the public sector?
An offence	Yes
A serious risk to public health, or public safety, or the health or safety of any individual, or to the environment	Yes
A serious risk to the maintenance of the law including the prevention, investigation and detection of offences or the right to a fair trial	Yes
An unlawful, corrupt or irregular use of public funds or public resources	Yes
Oppressive, unlawfully discriminatory, or grossly negligent or that is gross mismanagement by a public sector employee or a person performing a function or duty or exercising a power on behalf of a public sector organisation or the Government	Yes

Section 10 of the Act

5. Examples of Serious Wrongdoing:

5.1. While not an exhaustive list the following are examples of disclosures covered under this policy:

- failure to comply with legal obligations
- serious health & safety risks to an employee
- serious health and safety risks to the public
- unauthorised use of Council funds
- fraud, corruption or red flag tip-offs
- physical abuse
- damage to the environment
- unprofessional actions with the company or entity

6. How to escalate a concern of "Serious Wrongdoing"

6.1. Notify your manager immediately, or alternatively HBRC's P&C Manager who is assigned as HBRC's Protected Disclosure Act (PDA) Coordinator.

6.2. If the concern relates to your manager, then the concern should be reported to your Group Manager, or HBRC's P&C Manager (as HBRC's PDA Coordinator).

6.3. If the concern relates to your Group Manager, then the concern should be reported to the Chief Executive (CE), or alternatively HBRC's P&C Manager (as HBRC's PDA Coordinator).

6.4. If the concern relates to the CE, then the concern should be reported to the Chairman of Council (the Chair), or HBRC's P&C Manager (as HBRC's PDA Coordinator).

6.5. While staff are encouraged to report concerns of serious wrongdoing to their manager there maybe exceptional circumstances that anonymity is sought. In these circumstances HBRC has available a confidential protected disclosure line (also known as a whistle-blower line) that is managed independently by a third party, currently Crowe. That number is: (03) 474 5813, or mobile 021 773 018. Crowe will then provide the details of the information collected anonymously to HBRC P&C Manager in their capacity as HBRC's PDA Coordinator.

6.6. All concerns of serious wrongdoing escalated through the channels outlined in 6.1 - 6.5 above, are then protected under the Protected Disclosure Act by virtue of this policy. A disclosure to the media is NOT protected under the PDA 2022.

6.7. Any HBRC manager on receiving notification of potential serious wrongdoing must not:

- discuss the situation with anyone other than those mentioned in this policy, or
- attempt to investigate any concern of serious wrongdoing.

7. What happens after a concern of possible serious wrongdoing is raised?

7.1. The receiving manager you report your concern to will immediately notify:

- the CE, or where the concern relates to the CE, the Chair, and
- HBRC's P&C Manager (as HBRC's PDA Coordinator)

7.2. Concerns raised should be documented and if the criterion of serious wrongdoing is met this document, then becomes a *protected disclosure* in terms of the Act.

7.3. The CE or in the alternate case the Chair, may appoint an investigator or, in certain circumstances a law enforcement agency. The CE or in the alternate case the Chair should notify HBRC's external auditor if any serious wrongdoing meets the criteria of internal fraud (refer Internal Fraud Policy).

7.4. All concerns of serious wrongdoing will be acknowledged within 20 days of the disclosure. If the disclosure is not going to be investigated, then a reason 'why' must also be provided.

8. Gathering of Information

8.1. The receiver of protected disclosures must keep confidential information that might identify the discloser. The only exceptions are if the discloser provides written consent to the release that information. Or, if there are reasonable grounds to believe that the release of identifying information is essential:

- For an effective investigation
- To prevent serious risk to public health or safety, and individuals' health or safety, or harm to the environment
- To comply with principles of natural justice, or
- To an investigation of a law enforcement or regulatory agency for the purpose of law enforcement
- To the Local Government Official Information and Meeting Act 1987, requests must be declined if the request may identify the discloser.

8.2. The PDA Coordinator will:

- Listen to you fairly and with an open mind.
- Treat the information confidentially.
- Provide you with information and guidance on:
  - Helping you to identify all relevant factual information.
  - How you are protected under the Act.
  - What options you have if you are not satisfied with the result or with the time taken.
  - When you can approach others about this issue (clauses 8 to 10 of the Act).

9. **What can I do if I'm not happy with the outcome?**

9.1. The PDA Coordinator will explain the options for you to take this further if you are not satisfied - (Clauses 8 to 10 of the Act.)

10. Breach of policy – consequences of non-compliance

10.1. If you do not escalate your concerns as guided by this policy your concern may not be protected. In addition, this policy would be considered breached if:

- a party fails to keep confidential any concern covered by this policy, or
- the concern raised is not genuine

This type of breach may give rise to disciplinary action for serious misconduct.

Summary of key document changes and version control				
Version	**Date**	**Key changes to be communicated to staff**	**Document owner**	**Approver**
1.0	23/11/22	Full redraft to align with the Internal Fraud policy and protect fraud tip-offs. And the inclusion of a confidential whistle-blower line.	P&C Manager	Chief Executive
2.0	09/08/23	Updated the confidential protected disclosure line phone numbers	P&C Manager	Chief Executive

Policy

Title:	Privacy Policy
Policy number:	CD0029

Team policy owned by:	Legal	**Version number:**	4
Document owner:	Aimee Sandilands	**Date policy last reviewed and published:**	2025/10/14
Document approver:	Pip O'Connor	**Next review due:**	2026/10/14

Purpose

The purpose of this policy is to outline how Hawke's Bay Regional Council will comply, and have its employees and contractors comply, with relevant requirements of the Privacy Act 2020 ("Privacy Act") governing how HBRC collects, uses, stores and shares personal information.

Target audience

This policy applies to all Elected Members, Sub-Committee Appointees, Staff and Contractors of HBRC.

Policy details

1. **Policy goal or objective**

   1.1. Personal privacy is important to Hawke's Bay Regional Council (referred to in this Privacy Policy as "HBRC", "we", "our" or "us"). Therefore, this Privacy Policy governs collection, use, storage, access and disclosure of personal information (as defined in the Privacy Act) and has been prepared in accordance with the obligations and rights set out in the Privacy Act. This Policy guides HBRC's Policy Statement that is published on HBRC's website

2. **Related documents (e.g., Legislation, Policies, SOPs, etc)**

   2.1. Local Government Act 2002 and the Local Government Act Amendment Act 2014

   2.2. Local Government Official Information and Meetings Act 1987

   2.3. Privacy Act 2020

   2.4. Public Records Act 2005

   2.5. HBRC's Privacy Statement – Copyright and Privacy - HBRC website

   2.6. Acceptable Use Policy CD0002

   2.7. Motor Vehicle Use and Safe Driving Policy CD0011

   2.8. Lone Isolated Worker Emergency Alert Device Use Policy CD0012

   2.9. Policy Handbook CD0001

3. **Key definitions/abbreviations**

3.1. **Criminal Activity**: means any violation of the law where a person is liable to punishment for a criminal offence. A criminal act often threatens and harms public safety, property and/or welfare.

3.2. **Personal information** (sometimes called "personal data"): means any information about an individual (natural person) from which that person can be identified. The information does not need to name the individual, if they are identifiable in other ways, such as through their home address. It does not include data where the identity has been removed (anonymous data).

3.3. **Public Spaces**: spaces that are completely accessible to the public, such as tracks, regional parks.

3.4. **Privacy Officer**: a member of staff of HBRC who has been delegated the responsibilities under section 201 of the Privacy Act. Currently the Chief Legal Advisor.

3.5. The terms **include** and **including** do not imply any limit and are deemed to be followed by the words **without limitation**.

4. Types of Information Collected

4.1. Generally, the types of information collected by HBRC depends on circumstances in which information is collected. HBRC only collects personal information if it is for a lawful purpose connected with HBRC's functions or activities, and only to the extent the personal information is necessary for that purpose. Examples might include:

4.1.1. Date of birth

4.1.2. Physical or postal addresses

4.1.3. Email address

4.1.4. Telephone numbers

4.1.5. Age

4.1.6. Gender

4.1.7. Financial information

4.1.8. Banking details

4.1.9. Individual's picture

5. How Personal Information is Collected

5.1. Most personal information is collected directly or from someone authorised to act on behalf of, the individual. Examples of how personal information might be collected by HBRC include:

5.1.1. Applying for employment

5.1.2. Applying for consents, permits, funding etc

5.1.3. Corresponding in person, by letter, phone, text, email, instant messages or other means of electronic communication

5.1.4. Completing and submitting forms provided by HBRC

5.1.5. Using our online services and apps, such as our online payment services

5.1.6. Use of HBRC's website (or any other platforms)

5.1.7. Providing a written submission, request, or other feedback

5.1.8. Subscribing to any of our newsletter or update services

5.1.9. Public meetings

5.1.10. Using HBRC's social media or other facilities such as Facebook, Twitter, LinkedIn, YouTube, etc to follow or post comments

5.1.11. Participating in a promotion or competition carried out by HBRC or by a third party with official affiliation to HBRC

5.1.12. Participating in market research or surveys carried out by HBRC or by a third party on behalf of HBRC

5.1.13. Volunteering with a group related to HBRC

5.1.14. During a meeting that is filmed or recorded (with consent) (see further section 16.3 of this Privacy Policy, below)

5.1.15. On HBRC owned or licensed CCTV or camera footage (see further section 15 of this Privacy Policy, below)

5.2. HBRC also collects personal information from other organisations, entities, or persons. Including:

5.2.1. Land Information New Zealand

5.2.2. District councils

5.2.3. Registered valuers

5.2.4. The New Zealand Police

5.2.5. Credit reporting agencies

5.2.6. Other organisations, entities and persons when authorised them to do so

5.2.7. In a declared emergency and under the Information Sharing Code

5.3. By using HBRC's platforms and/or otherwise providing HBRC with information consent to use personal information will be in accordance with HBRC Privacy Statement that is published on HBRC's website.

6. Why HBRC Collects Personal Information and How HBRC Uses It

6.1. Personal information is only used for the purposes it was provided for and any other purpose that was informed at the time of collection.

6.2. HBRC does not use contact details for general marketing purposes.

6.3. Individuals can request to stop receiving correspondence from HBRC at any time unless information is required to comply with legislation or to perform HBRC's statutory obligations.

6.4. Examples of why HBRC might collect personal information include:

6.4.1. To provide necessary support in relation to interactions

6.4.2. To positively confirm identity (to avoid inappropriate release or use of your information)

6.4.3. To stay in touch regarding enquiries, comments, complaints or requests for information or services

6.4.4. Processing application for consents, permits, funding etc

6.4.5. Processing application for registration to HBRC services or to gain access to information on HBRC platforms that are made available only to registered users

6.4.6. To process payments either received or made by HBRC

6.4.7. To correspond for purposes such as consultation, market research and surveys

6.4.8. To provide products, services, or resources and to assist HBRC to provide such products, services or resources

6.4.9. To provide information about events, news, or services that HBRC considers potentially of interest

6.4.10. To administer and improve HBRC's platforms

6.4.11. To conduct a promotion or competition

6.4.12. To assess suitability for employment

6.4.13. To carry out activities connected with the running of our business or operations such as personnel training, or testing and maintenance of computer and other systems

6.4.14. To monitor HBRC assets (including stop banks, drains, and pathways) and natural features (including river mouths and regional parks) it is responsible for maintaining

6.4.15. To comply with relevant laws or legislation

7. Sharing of Personal Information

7.1. HBRC respects the privacy of personal information, therefore all reasonable safeguards are put into place to prevent its loss, misuse or unlawful disclosure.

7.2. HBRC may only disclose personal information when it is allowed to do so under the law. This includes that: (i) access to personal information is confined to authorised users only, which may include HBRC employees, contractors, and agents; and (ii) personal information without the individual's consent must not be provided to any third parties except:

7.2.1. To provide products or services, where that information is necessary for the provision of those products or services

7.2.2. To a Council Controlled Organisation in order to assist with the products and services that are provided to the individual

7.2.3. If authorised by the information owner to disclose their personal information

7.2.4. Where the information is going to be used in a way that could not identify the individual e.g., statistical reporting

7.2.5. To HBRC's lawyers, auditors, other professional advisors and contractors, but only to the extent necessary for the purpose of HBRC's engagement

7.2.6. To a third party if HBRC is required to do so under any laws or regulations, or during legal proceedings or other investigations e.g., CCTV recordings with the New Zealand Police or other public sector agencies where criminal activity is reported or suspected

7.2.7. To any person, if that information is held in a public register, e.g., information held on property files or the rating information database.

7.3. An authorised recipient of personal information held by HBRC shall only be entitled to use that personal information as strictly required for the purpose(s) for which it was provided to them.

8. Personal Information Storage, Accuracy and Security

8.1. HBRC takes reasonable steps to ensure personal information is:

8.1.1. Protected against loss, damage, misuse and unauthorised access or disclosure.

8.1.2. Access to personal information is restricted to those individuals who need access to this information to perform our duties and obligations

8.1.3. Accurate, up to date, complete, relevant, and not misleading.

8.2. Personal information may be stored electronically/digitally and/or in paper form.

8.3. HBRC may provide passwords or other security devices via which authorised persons may access personal information within the scope of this Privacy Policy. When doing so HBRC must advise the individual of the importance of keeping passwords confidential and not allowing devices to be used by any other person.

8.4. Any breach or potential breach involving personal information, must be escalated immediately to HBRC's Privacy Officer (Chief Legal Advisor) (and may be required to be notified to the Privacy Commissioner).

9. Retention of Personal Information

9.1. HBRC must only keep personal information for as long as is necessary to achieve the purpose(s) for which it was collected, taking into consideration any continued support required, administrative requirements, or contractual and legal obligations.

9.2. The Public Records Act 2005 requires HBRC to retain "protected records" indefinitely. In some circumstances, personal information may be included within a protected record, including submissions in relation to bylaws, annual plans, and regional planning instruments.

10. Access to and Correction of Personal Information

10.1. Under the Privacy Act individuals generally have the right to:

10.1.1. Obtain confirmation on whether or not HBRC holds personal information about them.

10.1.2. Request access to personal information held.

10.1.3. Request correction of that personal information if it is incorrect, out of date, misleading or incomplete.

10.2. HBRC will provide access to your personal information unless required or authorised to refuse such access by law. In some cases, individuals may be charged for retrieving and providing a copy of their personal information. If this is the case, advice of charges must be confirmed, and payment may be requested, prior to HBRC making the disclosure.

10.3. If HBRC is entitled to refuse the request to correct personal information, the individual will be notified with information required to be given with that notification included.

11. Automated Data Collection Technologies

11.1. HBRC and HBRC's Platform providers use automatic data collection technologies to store some information such as 'cookies'. Cookies provide details of IP address, operating system, browser, search terms, pages accessed, and links clinked, dates and times of visits, immediate previous site visited, and domain. Information generated by cookies aims to personalise the website experience with better tailored information. Platform providers may also make a record of website visits and log information for statistical purposes

11.2. Visitors to HBRC's website must be able to refuse cookies by turning them off in the browser and deleting them on hard drives.

11.3. Cookies must not be used by HBRC to extract any personal information.

11.4. HBRC may allow analytics services to be provided by others e.g., Google Analytics. This information must be aggregated so users are anonymous and not personally identifiable. This statistical information will be viewable by website administrators and certain other HBRC employees and contractors.

12. Call Recording

12.1. HBRC is committed to providing the best possible service to our customers, therefore calls may be monitored and recorded to the HBRC 0800 number (0800 108 838) and the main phone line at each HBRC location for the following purposes:

12.1.1. for quality control and staff training to improve HBRC's service and to ensure that the information provided is consistent and accurate

12.1.2. to keep an accurate record of calls

12.1.3. for other purposes related to the call.

12.2. HBRC must let all parties know at the time of the call if a call is to be or may be monitored and recorded and the purpose and use of such recordings.

12.3. Any personal information provided as part of the call must be managed in accordance with this Privacy Policy.

13. Links to External Websites

13.1. HBRC may provide links to third party websites or digital services. If this is the case HBRC must on the website provide a statement that HBRC's Privacy Policy and standards do not apply in these circumstances and that HBRC has no responsibility for (amongst other things) how those external linked websites or services handle personal information.

14. Mobile Applications

14.1. HBRC's mobile applications, must provide a statement so that the user acknowledges and accepts in doing so HBRC can:

14.1.1. send 'Push Notifications' any time. 'Push Notification' preferences should be configurable in the application's settings, including the ability to disable the notification.

14.1.2. access the device's location function and collect, use, and disclose this information as set out in this Privacy Policy. Share location must also be able to be disabled in the settings.

15. Surveillance Cameras (Fixed or Aerial)

15.1. **Purpose:** Surveillance cameras including "Closed Circuit Television" (CCTV), still cameras and drones which make recordings or take photos and which may capture personal information (together, "**Surveillance Cameras**") are used for legitimate purposes connected with HBRC's functions. This includes securing HBRC's facilities, assets and services to:

15.1.1. improve safety for staff, contractors, elected members, visiting public etc

15.1.2. deter potential vandalism and damage of any HBRC asset

15.1.3. use, where appropriate, for law enforcement purposes

The above includes that Live streaming CCTV Surveillance Camera footage of public places by HBRC is restricted to locations and situations where it is for legitimate purposes, for example to monitor weather, floods or river levels or for public emergency or other operational purposes.

15.2. **Signage:** Signage advising of use of Surveillance Cameras by HBRC in an area will be clear, give the required notice of Surveillance Cameras operating and provide other information as may be necessary.

15.3. **Positioning:** Surveillance Camera coverage will not be positioned in a way that intrudes to an unreasonable extent on the privacy of individuals, for example, it is not intended to capture footage of:

15.3.1. those areas of HBRC assets which individuals would reasonably expect to be private for example the inside of toilets or changing rooms; or

15.3.2. private property except unavoidably as part of a wide angle or long shot while panning past.

15.4. **Use:** Surveillance Camera footage will only be used and disclosed for lawful purposes, including in accordance with the original purpose for which it was installed or for the purpose of regularly checking the system is operational.

15.5. **Access, retention and other management:** Access, retention and other aspects relevant to personal information in CCTV Camera footage will be managed in accordance with this Privacy Policy.

16. **Other Visual Media**

16.1. HBRC may collect and use personal information in the form of other visual media, for the following purposes:

16.1.1. For use in various documents on the website, including planning documents, maps and promotional material

16.1.2. To monitor the state of HBRC assets

16.1.3. For operational purposes, including monitoring and responding to public emergencies

16.1.4. To monitor compliance with regulations and central government legislation, e.g., the Resource Management Act

16.2. Managing Other Visual Media: We will only publicly disclose and/or use such other visual media where we have the consent of the individuals identifiable in it (or public disclosure and/or use is otherwise lawful in the circumstances). Other visual media be stored, accessed and otherwise managed in accordance with this Privacy Policy.

16.3. HBRC may record Council meetings for the following purposes:

16.3.1. To provide an accurate verbatim record of meetings

16.3.2. For providing public access to meetings

16.3.3. For quality control or employee training purposes

16.3.4. If meetings are to be recorded and if, applicable, being live streamed, this information will be provided at the time of the meeting and HBRC will inform attendees of the meeting before the meeting starts (serving as implied consent regarding personal information of those who remain)

17. **Breach of policy – consequences of non-compliance**

17.1. The HBRC Chief Legal Advisor is responsible for monitoring compliance with this policy. Failure to comply may be considered misconduct and may result in disciplinary action, up to and including termination of employment.

Summary of key document changes and version control

Version	Date	Key changes to be communicated to staff	Document owner	Approver
1.0	11/5/23	New policy – to be communicated to all staff via Snappy and with the Privacy ABC training	Risk Manager until Legal Counsel Appointed	Group Manager Corporate Services
2.0	02/05/24	Annual review, change of document owner until Risk Manager role replaced	Quality & Assurance Advisor	Group Manager Corporate Services
3.0	21/07/25	Annual review: Changes to reflect recent internal staffing updates (Privacy Officer, Team policy ownership, document owner, document approver); Changes to align more accurately with Privacy Act; Changes aiding clarity/interpretation of requirements; Some improvements to camera surveillance (including CCTV) section	Chief Legal Advisor	Acting Group Manager Corporate Services

Policy

Title:	Gifts, Hospitality and Winnings Policy
Policy number:	CD0005

Team policy owned by:	Risk and Assurance	**Version number:**	3
Document owner:	Helen Marsden	**Date policy last reviewed and published:**	2025/06/10
Document approver:	Susie Young	**Next review due:**	2027/06/10

Purpose

The purpose of this policy is to maintain stakeholder confidence in the HBRC by providing an impartial, transparent and consistent means for HBRC staff and affiliates to accept or decline and record offers of gifts, hospitality and winnings from a third party to HBRC.

Target audience

This policy applies to all HBRC elected members, sub-committee appointees, staff, and contractors of HBRC.

Policy details

1. Policy goal or objective

1.1. The goal of this policy is to provide clarity to HBRC staff and affiliates who through their engagement with HBRC might be offered a gift, hospitality or prize (winnings) from a third party to HBRC. By, setting out the principles that must be applied when considering whether to accept or decline offers of gifts, hospitality or winnings.

2. Related documents

- Internal Fraud Policy - CD0003
- Conflicts of Interest Policy - CD0004
- Protected Disclosures Policy – CD0006
- Procurement Policy - CD0007

3. Key definitions/abbreviations

3.1. **Affiliates** - means HBRC elected members, sub-committee appointees, staff, and contractors, of HBRC.
Bribe - means a gift or benefit that is offered to or solicited by an employee in order to influence that person to act in a particular way.
Gift - means rewards, gratuities, or items of monies given by a third party beyond remuneration and reimbursement. Examples of gifts include goods (such as money, tickets, vouchers, manufactures samples), or services (such as free use of a corporate box at a sporting event or privileged access to goods or services).

Gift register is the online register on Kowharawhara under 'I want to...' for recording offers of gifts, hospitality and winnings.

Hospitality - means any item or service provided by the third party to be consumed at the meeting or function (e.g., food, drink, transportation, preferential treatment, accommodation, discounted conferences or training). If you are representing HBRC in an official capacity at a function this is not considered hospitality for personal benefit but part of your employment.

Third Party – is any individual or organisation other than HBRC, whether public or private sector. When a third party has different business models that segregates different business products and services or national boundaries, these can be treated as different third parties.

Winnings - are things that you are given as a prize (e.g., random draws, lucky door prizes, merit-based prizes etc).

1. Introduction

1.1. All HBRC staff and affiliates are required to be fair, impartial, responsible and trustworthy, and act in a way that maintains public confidence. From time to time a staff member as an employee of HBRC and other HBRC affiliates may directly be offered or receive a reward in the form of a gift, hospitality or winnings from a third party of HBRC.

1.2. In all cases staff and affiliates must be very careful about accepting gifts, hospitality or winnings and always be aware of the public perception that can result from accepting these.

2. General Principles

2.1. This policy aims to ensure that when gifts, hospitality or winnings are offered, they are managed in a fair and transparent manner that protects the reputation of HBRC, HBRC's staff and HBRC's affiliate. As set out by the Office of the Auditor General, receiving a gift, hospitality or winnings from a third party is a sensitive issue, and one that needs to be managed carefully.

2.2. The general policy position is that gifts, hospitality and winnings **will not** be accepted unless the gift has a value less than $250. Or, in the case of more than one offer by the same third party over any 12-month period a cumulative value of less than $250. Or, where refusal would cause cultural or diplomatic embarrassment or offence. However, there are certain circumstances where even modest offerings **must be** declined (refer section 4 of this policy – under *'Practice')*.

2.3. As a matter of guidance even modest offers of gifts, hospitality or winnings must be infrequent. Where any gift, hospitality or winnings are offered and accepted from the same third party over any 12-month period with a cumulative value of $100 or more these should be treated the same as single offerings of $100 or more. Likewise, any gift, hospitality or winnings that are offered and accepted from the same third party over any 12-month period with a cumulative value of $250 or more should be treated the same as a single offering of $250 (refer section 3 of this policy – under table 1 *'Thresholds'*).

2.4. All offers of gifts, hospitality or winnings with a cumulative value of $100 or more over any 12-month period from the same third party **must be** approved by the Group Manager, or in the case of the Group Manager the Chief Executive (CE), before accepting and recording the offer into HBRC's gift register located on Kowharawhara, under …. *I want to*…. The HBRC staff member or affiliate who is offered the gift, hospitality or winnings is responsible for recording the offer into the register. If they do not have access to the on-line register, they must request in writing that the line manager they report to or the manager who oversees their relationship with HBRC record the offer into the register on their behalf. The CE, Elected members or Sub-committee appointees must advise in writing either the CE's Executive Assistant (EA) or a member of HBRC's Strategy and Governance Team who will record the offer into the register on their behalf.

2.5. If in doubt about accepting gift, hospitality or winnings, seek guidance from your manager.

2.6. This policy applies in all circumstances including where gifts, hospitality or winnings is offered outside normal working hours or while on leave but through your relationship with HBRC.

3. Threshold

3.1. The table below outlines threshold criterion for dealing with or accepting offers of gifts, hospitality, or winnings:

Table 1: Thresholds

Offer of a Gift, Hospitality or Winnings	An offer or offers from the same party with a cumulative nominal value of less than $100 over any 12 months	An offer or offers from the same party with a cumulative value of $100 but less than $250 over any 12 months	An offer or offers from the same party with a cumulative value of $250 or more over any 12 months
Approval	• Use personal judgement on whether to accept or not. Refer to section 4 – *Practices* - in this policy for types of offers that **must be** declined regardless of the cumulative value.	• Group Manager, or for Group Managers CE, approval required prior to accepting the offer. • In the case of the CE and Councillors continue to apply personal judgement on whether to accept or not. Refer to section 4 – *Practices* - in this policy for types of offers that **must be** declined regardless of the cumulative value. • For those affiliated with Council but not a direct employee approval is required from the Group Manager of the Group that holds the main relationship with the affiliated party.	• Consider declining the offer unless the refusal would be culturally offensive or embarrassing. • CE approval is required in writing prior to accepting the offer. • CE requires HBRC Chair approval prior to accepting the offer where the accumulative amount (based on the latest gift) would reach above $250. • Councillors require HBRC Chair approval prior to accepting the offer.
Recording and Handling	• No entry is required into the gift register; however, staff may enter into the register if they wish to for full transparency.	• The Group Manager or in the case of the Group Manager the CE, may: approve the acceptance of the offer, decline to accept, or return the gift.	• If the gift or winnings are accepted the CE or HBRC's Chair may require that these be surrendered to HBRC for suitable disposal (refer section 6 of this policy – Declining or

		• All offers are recorded in the register regardless of whether the gift, hospitality or winnings have been accepted or not AND note any disposal actions taken.	disposing of gifts, hospitality, or winnings). • Record in the register if the gift, hospitality, or winnings have been accepted or not AND note any disposal actions taken.
Exceptions	• Air points earned on company trips • Approved P&C discounts available to all employees • Meals provided: at a networking, business or planning meeting, or site visit, a function or gathering such as a presentation to a community group, or a conference, training exercise or course**.**		

4. **Practice**

4.1. Unacceptable gifts, hospitality and winnings

- Gifts, hospitality, or winnings **must always** be declined regardless of amount in the following circumstances:
  - Money, cash vouchers, shares, personal discounts or similar items and payments.
  - That might compromise or be seen to compromise, your integrity as a HBRC employee or affiliate.
  - When the HBRC staff or affiliate seeks out gifts, hospitality, or winnings.
  - Where direct instruction has been given by the Group Manager, Chief Executive, or Chair that the offer **should not** accepted.
  - Where acceptance could be perceived as a promise of a business relationship or contract.
  - Where the value of the gift, hospitality or winnings offered is out of keeping with an acceptable norm.
  - Where acceptance is a strong indication that preferential treatment is expected.
  - Are offered immediately prior to, or during, a consent application and/or pre application process by any party involved in that process.
  - During a procurement, tendering or similar situation where HBRC is likely to be making decisions involving the third party offering the gift, hospitality or winnings, and
    - The offer is made at a time close to, or during a procurement, tendering, or similar process.
    - Can be seen as an inducement or reward which might place an obligation to a third party including a panel of preferred providers.
  - In cases of continuous procurement, such as an ongoing panel of preferred suppliers, it is unacceptable to accept gifts, hospitality or winnings during the time that the panel is

being established or reviewed, or when providers are under consideration for specific jobs.

- If any doubt remains, you should err on the side of caution and decline the gift or hospitality.

4.2. To assess whether to accept modest offers of gifts, hospitality or winnings not covered by section 4.1, consider:

- how a reasonable member of the public, having only a general understanding of the HBRC's business and interests, might view accepting that gift/hospitality. This will include, but is not limited to, an assessment of:
  - the perceived value and nature of the gift, hospitality or winnings.
  - the perceived personal benefit obtained.
  - whether the public might have cause to think there is a conflict of interest (whether actual or perceived).
  - whether the public might have cause to think that the HBRC staff member or affiliate may become improperly influenced or obliged.
  - frequency including any patterns of offerings.
  - the timing of the offer.
  - the proportionality between the offer and HBRC's business benefit.
  - the nature of the relationship between the HBRC staff member or affiliate and the third party, and
  - the potential for the situation to be misconstrued by the public if accepted.

5. Gift Register

5.1. A gift register is maintained to keep track of gifts, hospitality and winnings offered for all cumulative amounts of $100 or more from the same third party over any 12 months.

5.2. B**efore** accepting the offer and updating the register approval must be provided as outlined in section 3: Thresholds - Table 1 of this policy.

5.3. The Register will be available for viewing by HBRC staff.

5.4. The following information will be captured on the Gift Register:

- Received by (name and title)
- Group
- Date received
- Date recorded
- Third Parties name providing the offer
- Gift item/benefit and description
- Occasion or reason for the offer
- Estimated value
- Whether the gift, hospitality or winnings were Accepted or Declined – reasons why

- If the gift is accepted, how the gift is being dealt with, including any disposal.

5.5. The Gift Register is overseen by the Risk and Corporate Compliance Team Leader. New records in the gifts register are reported to ELT on a quarterly basis.

6. **Declining OR disposing of gifts, hospitality or winnings**

6.1. Where it is not considered appropriate to accept a gift, hospitality or winnings it should either be politely refused (if offered directly). Or, be returned to the sender with a polite note thanking the sender for it and advising them that the acceptance is not appropriate under HBRC's policy.

6.2. There will be times when it is inappropriate to either decline or return a gift, hospitality, or winnings e.g., for cultural reasons. In these cases, the Group Manager in consultation with the CE will determine what will happen with it. This may include, but is not limited to:

- donating the gift to a suitable charity or organisation.
- disposing of the gift in an alternative way that would not offend the giver.
- the item being made a Council asset and added to the asset register.
- donating it to the social club.
- donating the gift to the social club for a raffle or social function.

6.3. Declined offers of gifts, hospitality or winnings should still be noted as such in the gift register.

4. Breach of policy – consequences of non-compliance

This policy would be considered breached if you as a HBRC staff or affiliate do not accept, decline or register any offer of gifts. Hospitality or winnings in accordance with this policy. A breach of this policy may give rise to disciplinary action for serious misconduct.

Summary of key document changes and version control

Version	Date	Key changes to be communicated to staff	Document owner	Approver
1.0	02/11/22	Full redraft including clearer thresholds and criteria for accepting or declining gifts. And a gift register declaration form accessible to staff through Kowharawhara "I want to….." This policy supersedes SP0018.	Helen Marsden	Susie Young
2.0	29/10/2024	Annual Review – small amount of grammar changes and job title.	Olivia Giraud-Burrell	Susie Young

POLICY

Title:	Media
Policy number:	CD0064

Team policy owned by:	Communications and Engagement	**Version number:**	1
Document owner:	Mike Johansson	**Date policy last reviewed and published:**	2025/10/06
Document approver:	Te Wairama Munro	**Next review due:**	2027/10/06

Purpose

The purpose of this policy is to ensure:

- Positive, proactive media coverage of relevant Council projects, programmes and general operation
- A consistent, streamlined approach to managing media
- Appropriate authorisation of Council messages
- Delivery of accurate of information and consistent messaging
- Responses are provided to media in a timely manner

Target audience

This policy applies to all staff, elected members, and contractors working for Hawke's Bay Regional Council who may at some point be in a position to make a public communication via the media

Policy details

1. **Policy goal or objective**

   1.1. Hawke's Bay Regional Council has a clear goal of delivering excellent service to the people of Hawke's Bay.

1.2. To do this effectively, it is important all residents and ratepayers have confidence in what we do and the decisions we make. They have a right to know how their rates are spent, and we have a responsibility to keep them informed.

1.3. Communication with the public should be open, responsible and timely.

1.4. The media is one avenue through which we can achieve this.

2. **Related documents (e.g. Legislation, Policies, SOPs, etc)**

2.1 Hawke's Bay Regional Council's Communications Strategy

2.2 Hawke's Bay Regional Council's Social Media Policy

2.3 Any Communications Strategy or Plan relating to an area of Regional Council operation

2.4 Hawke's Bay Regional Council Staff Code of Conduct

3. **Key definitions/abbreviations**

3.1. **Media** - all channels, platforms, and formats used to create, publish, and distribute information, news, or entertainment to a public audience, including both professional/commercial organisations and independent or user-generated sources.

3.2 **Public Communication/Opinion** – Any message, content, or information intended for, or accessible by, the general public or a broad audience outside the organisation. This includes communications via mass media, social media, websites, public reports, advertising, speeches, blogs, and any forum where access is not restricted.

4. **Designated Media Spokespeople**

4.1 Generally, only the Chair, the Chief Executive, Group Managers, the Director of Communications & Engagement and the Team Lead Communications (or their designees) will represent the organisation and respond to the media on behalf of the Council.

4.2 Only Regional Council employees designated as spokespeople in their area of expertise and who have undergone appropriate media training should be responding to the media.

4.3 They must adhere to the steps outlined below when dealing with media. This ensures consistent messages across the organisation and helps to keep track of media enquiries.

4.4 The Executive Leadership Team will decide on the designated spokespeople within their groups. Staff should check with Comms & Engagement and/or their Group Managers to see if it is appropriate for them to speak to the media.

5. Media contact

5.1 All approaches by media to staff should be notified to the Comms & Engagement Team. A team member will work with staff member to determine the best response and the level of response.

5.2 If media contacts the Comms & Engagement Team directly seeking answers to questions or an interview this will be directed to a GM or subject matter expert (SME)

5.3 The GM or SME will do their best to answer the inquiry in the shortest practicable time and then the Comms & Engagement team member will respond to the media.

5.4 Staff, elected members or contractors may from time to time wish to offer opinions to media in print, on air or online and as private citizens they may do this so long as they do not claim to

represent the Hawke's Bay Regional Council in these communications. As a courtesy they should alert the Comms & Engagement Team under the guiding principle of "no surprises."

5.5 Should staff, elected members or contractors wish to offer opinions to media in print, on air or online and make their association with Council a clear part of these communications it will be a decision by the CE (staff), the Chair (councillors) or the appropriate GM (contractors) as to whether this is an appropriate or permissible activity.

6. Breach of policy – consequences of non-compliance

6.1 Failure to follow this policy could lead to disciplinary proceedings

5.

Summary of key document changes and version control				
Version	**Date**	**Key changes to be communicated to staff**	**Document owner**	**Approver**
1		Transferring SP043 into Controlled Document systems and update; added Media contact (section 5); updated Key definitions (section 3) and breach of policy (section 6)	Mike Johansson	Te Wairama Munro

POLICY

Title:	Social Media
Policy number:	CD0065

Team policy owned by:	Communications and Engagement	**Version number:**	1
Document owner:	Mike Johansson	**Date policy last reviewed and published:**	2025/10/06
Document approver:	Te Wairama Munro	**Next review due:**	2027/10/06

Purpose

This policy sets out how Hawke's Bay Regional Council staff use social media in both their professional and personal capacities. It aims to:

- Support open, respectful and constructive engagement with our communities.
- Protect the reputation, integrity, and legal standing of the organisation.
- Provide guidance for responding to risks, negative activity, or crisis situations online.

Target audience

This policy applies to:

- All staff, contractors, and elected members acting on behalf of Hawke's Bay Regional Council.
- Staff engaging on their own personal social media channels, where their behaviour could reflect on the organisation.

Policy details

1. **Policy goal or objective**

The objectives of this policy are to:

1.1 Ensure Hawke's Bay Regional Council maintains a consistent, professional, and trustworthy presence on all official social media channels.

1.2 Provide staff with clear expectations for personal and professional use of social media.

1.3 Ensure responses to negative activity or crisis situations are timely, coordinated, and aligned with best practice.

1.4 Safeguard staff, the organisation, and the public from harm caused by inappropriate or unlawful online behaviour.

2. **Related documents (e.g. Legislation, Policies, SOPs, etc)**

- The HBRC Social Media Guidelines

3. **Key definitions/abbreviations**

3.1. **Official Council social media:** Accounts administered by the Communications & Engagement Team on behalf of Hawke's Bay Regional Council.

3.2. **Personal social media:** Accounts operated by staff in their private capacity.

3.3. **Negative activity:** Content that is critical, hostile, misleading, defamatory, or harmful towards the organisation, staff, or community.

3.4. **Crisis:** An event or issue generating significant public concern that may damage the organisation's reputation or require urgent communication.

3.5. **C&E:** Communications and Engagement Team.

4. **Social media principles and staff responsibilities**

4.1. **Professional use**

4.1.1. Only the C&E Team (or those delegated) may post to official Hawke's Bay Regional Council social media channels.

4.1.2. Content must be accurate, timely, inclusive, accessible and respectful.

4.1.3. Posts must align with organisational priorities, branding and tone.

4.1.4. Records of official posts and interactions must be retained to meet public record obligations.

4.2. **Personal use -** Staff are free to use personal social media, but:

4.2.1. Staff must not disclose confidential or sensitive council information.

4.2.2. Staff must not use offensive, discriminatory or defamatory language.

4.2.3. Staff must make clear when expressing personal views that they are not speaking on behalf of the organisation.

4.2.4. Staff must be mindful that public comments may still be linked to their role at Hawke's Bay Regional Council.

4.2.5. Staff must be mindful that any social media accounts they launch or administer cannot represent a conflict of interest with their work for Council.

4.3. **Responding to negative activity**

4.3.1. The C&E Team will monitor official channels for negative activity.

4.3.2. Where appropriate, correct misinformation calmly and factually.

4.3.3. Escalate legal, defamatory, or threatening comments to the appropriate authority.

4.3.4. Inappropriate comments (e.g. offensive, racist, abusive) may be hidden/removed in line with Hawke's Bay Regional Council's social media moderation guidelines.

5. **Breach of policy – consequences of non-compliance**

Non-compliance with this policy may result in:

5.1. Removal of social media privileges.

5.2. Formal disciplinary action in line with Hawke's Bay Regional Council's HR policies.

5.3. Referral to external authorities in cases of unlawful behaviour (e.g. breaches of privacy, harmful digital communications, or defamation).

Summary of key document changes and version control				
Version	**Date**	**Key changes to be communicated to staff**	**Document owner**	**Approver**
1	16/09/25	Policy rewritten to reflect changing expectations on staff use of social media outside of the work and responsibilities for social media for those doing that mahi art HBRC	Mike Johansson	Te Wairama Munro

Policy

Title:	**Risk Management Policy**
Policy number:	CD0023

Team policy owned by:	Risk and Assurance	**Version number:**	2
Document owner:	David Nalder	**Date policy last reviewed and published:**	2025/05/11
Document approver:	Susie Young	**Next review due:**	2026/05/11

Purpose

The purpose of this Policy is to set out HBRC's expectations and approach to risk management across the organisation. It provides the *'what, why and who'* for risk management within HBRC.

The appendix to this Policy describes HBRC's Risk Management Framework and provides guidance for staff as to *'how and when'* policy expectations might be met in practice.

The vision is for an integrated approach to risk management across HBRC, that reflects and supports the responsibilities and accountabilities of all those within the organisation to make good risk-aware decisions.

This policy aligns with principles of good governance and is intended to support informed decision making.

Target audience

This policy applies to all HBRC staff, contractors, elected members and sub-committee appointees.

Policy details

Policy statement

Risk is *'the effect of uncertainty on objectives'*.

Hawkes Bay Regional Council (HBRC) will proactively and explicitly manage risk to support the successful achievement of our objectives and commitments. This requires that all those within HBRC have a responsibility for ensuring that risk (i.e. the effect of uncertainty on the objectives of HBRC) is appropriately considered as part of the work they do and the decision they make.

The objectives of this policy are to:

- Enable Councillors and Management to bring an understanding of the major areas of uncertainty/risk inherent within decisions and commitments made and activities undertaken
- Ensure that there is a transparent link between 1) HBRC's priority objectives 2) uncertainty/risk that might impact these objectives 3) how this risk is managed through control 4) how confidence is obtained that controls are effective
- Build a risk-aware culture and enabling all staff to understand their specific roles and accountabilities in this regard
- Integrate 'risk management' approaches into core 'management' approaches, for that risk management just becomes good management – i.e. looking and securing upside opportunities, while minimising downside threats, related to the core commitments, obligations and work of HBRC

Accountabilities, roles and responsibilities

The following are the minimum mandatory expectations of all those within HBRC:

1. must identify and manage uncertainty/risk relevant to their role, area of responsibility and decision making
2. must document and manage material risks in accordance with HBRC Risk Management Framework
3. must ensure risks within their area of accountability are appropriately managed through core operational activities, processes, systems and internal controls
4. must report and escalate material risks (areas of uncertainty) and issues (risk events/incidents/problems that have occurred) on a timely basis
5. must read, understand and abide by HBRC's organisational policies, which set expectations and standards to guide action and decision making
6. must report and escalate circumstances where HBRC's policy expectations have not been met, which presents material risk to the organisation

Broadly, the following accountabilities are in place:

Council (elected members)	The Council of elected members is accountable overall for: • setting the strategic direction of HBRC and governance over the operations of HBRC that delivers on these strategic priorities and commitments • ensuring that there is a clear view of the level of uncertainty/risk that is appropriate, balanced to cost and benefit (risk appetite), to achieve the strategic direction of HBRC • Set specific governance accountabilities associated with risk management i.e. the role performed by the Risk and Audit Committee
Risk and Assurance Committee	The Risk and Audit Committee is accountable for undertaking its role as outlined in its Terms of Reference. Specifically, this includes accountability for: • Ensuring there is an effective and enduring approach to risk management, including for the identification, assessment, evaluation, mitigation, monitoring and reporting • Providing governance guidance on areas of significant risk/uncertainty
Chief Executive	The Chief Executive, together with the Executive Leadership Team, is accountable for delivery of day-to-day operational activities aligned with the strategic direction set by Council. This includes: • Promoting a risk aware culture, linking risk/uncertainty with decision making and action • the effective identification and management of risk (uncertainty) associated with these operations (operational risk), change initiatives (project risk) and overall achievement of strategic priorities (strategic risk) • ensuring Council (and the Risk and Audit Committee) understand the key areas of risk/uncertainty inherent with key objectives, decisions, initiatives and obligations • escalating any significant risks or concerns on a timely basis

All those within HBRC	Managers, staff, contractors and elected members are accountable for the effective delivery of business functions, activities, projects, initiatives and tasks aligned with HBRC's purpose, plans, priorities and commitments. This includes understanding and managing the risk (uncertainty) associated with this as part of the work they do
ELT leads	For each HBRC-wide strategic risk identified, a member of the Executive Leadership Team will be nominated as a 'lead' for this risk/uncertainty. The accountability for this role is to: • ensure that this area of risk/uncertainty is adequately defined in terms of causes, consequences, controls and monitoring measures • nominate a 'business owner' and work with this person to enable a whole-of-HBRC approach to managing this risk/uncertainty • ensure there is good visibility of the risks they lead and that this is explicitly drawn out in decision making
Business Owner	The Business Owner is accountable for working with the ELT Lead to ensure that these risks/uncertainties are effectively defined, assessed and managed across the Council. This includes accountability for ensuring: • associated risk plans are clear and up to date • controls and mitigation are effective • defining measures/metrics such that risk reporting can be integrated into wider organisational performance reporting
Risk Manager	The Risk Manager is accountable for supporting the those above (Councillors, the CEO, ELT, managers and staff) in achievement the above through a implementing and maintaining a consistent and enduring approach to risk management

All staff, particularly those with operational leadership and business unit accountabilities are required to explicitly consider the risks/uncertainty inherent with the business unit, activity, project or process they are accountable for.

This requires the following steps and questions to be considered:

1. **Risk context:** What are our objectives? Who are we accountable to and for what? What is the environment we are operating in? What does 'success' look like?
2. **Risk identification**: What might happen (i.e. specific risks/uncertainties) – both good (opportunity) and bad (threat)? What contributes to this (i.e. causes)? Why does this matter (i.e. consequences)
3. **Risk analysis**: How confident or concerned are we about this (i.e. the likelihood of this risk/uncertainty occurring and impact on HBRC should this occur)?
4. **Risk evaluation**: Can we live with this? Does this sit within or outside our agreed appetite/comfort zone as an organisation?
5. **Risk treatment**: What can and will we do about this?
6. **Risk monitoring and review**: How is this risk/uncertainty tracking? Are we managing this effectively?
7. **Risk reporting**: Who needs to know? What do we need to escalate and report? To whom and when?

Councillors, managers and staff have flexibility as to how they achieve this, but the policy expectation is that the above risk management steps will be performed, related questions considered, and results documented.

In the Appendix to this policy, guidance is provided as to how this might be achieved.

Two approaches are provided for:

1. A top down approach for considering whole-of-HBRC wide **strategic** risks
2. A bottom up approach for considering business function or activity specific **operational** and **project** risks

Strategic vs operational/project risk management approach

Risks will be identified on both a 'top down' and 'bottom up' basis.

1. ***Top down*** (i.e. strategic risk approach): defining 'risk' in terms of major areas of uncertainty related to HBRC's core purpose and definition of success

2. ***Bottom up*** (i.e. operational risk approach): defining 'risk' in terms of uncertainty relating to HBRC core operational processes, projects, initiatives and service delivery activities

In this respect the distinction between strategic and operational risk management is:

Nature	Strategic risk	Operational / project risk
Focus	Uncertainty/risk impacting HBRC's core purpose and strategic priorities	Uncertainty/risk impacting day to day operations, specific project and service delivery
Time horizon	Long term, aligned to the time horizon of the Long Term Plan and related strategic plans	Short term, aligned to operational business plans / project plans
Volume and volatility	A relatively small number of overarching themes. Reasonably consistent day to day, largely impacted by external factors and changing stakeholder expectations	A relatively large number of specific things. Reasonably changeable day to day
Reflected in	The HBRC Dashboard and supporting One Page Management Plans	Risk registers or equivalent documentation for specific functions, business units and projects

Irrespective of the nature of risk (i.e. whether it is a strategic, operational or project-based risk), those who are accountable for specific business areas, functions, activities and projects are accountable for effectively identifying, assessing, treating, monitoring and reporting the major areas of risk/uncertainty related to the areas they are accountable for.

Incident and issue management

An 'incident' or 'issue' is a problem or event that occurs when a 'risk' crystalises – i.e. something that might happen, has happened. This might be positive (a beneficial opportunity) or negative (a detrimental threat).

Where this is material – i.e. could significantly impact on HBRC in terms of it's reputation, legal or regulatory compliance, operational performance, stakeholder relationships, financial performance or similar, all staff must escalate these incidents/issues to their line manager, Risk Advisor and/or Chief Legal Advisor.

High Risk Incidents should have the appropriate Post Incident Implementation Report completed to identify learnings and enhancements required to business process.

Medium and High Risk Incidents must be reported through to the Risk and Audit Committee for awareness.

Appendix 1: Guidance for how to apply this Risk Policy

What is 'risk'

Risk is *'the effect of uncertainty on objectives'*.

Good risk management enables an effective understanding of uncertainty (i.e risk) relating to HBRC's purpose, priorities, objectives and activities.

This uncertainty may result in upside opportunity or downside threat.

The objective of risk management is to enable a linkage between, and address the following questions:

1. What is our purpose, vision and objectives?
2. What does 'success' look like?
3. How do we deliver on this?
4. What are the main areas of uncertainty that relate to this (risk)?
5. What upside opportunities or downside threats come from this uncertainty/risk?
6. What are the key drivers/causes of this uncertainty (sub-risks)?
7. How are we managing this (controls)?
8. How to we know that these activities/controls are effective?
9. What level of uncertainty/risk can we live with (risk appetite)?
10. How do we monitor our performance and whether we are within or outside our risk appetite?
11. What do we need to decide or do, as a result of the above?

Collectively, addressing the above questions provides a direct link between objectives, risks, controls, assurance and decision making.

In the context of this policy, every reference to *'risk'* should be considered as *uncertainty*, including both upside opportunity and downside threat.

Policy principles

The following eight principles underpin HBRC's expectations and approach to risk management:

Executive commitment	That the risk approach is visibly endorsed and driven by the executive – i.e., lead from the top with the leadership walking the talk
Clear accountability	That there are specific (single point) accountabilities assigned to do the work required – at the executive and management level, not just the Risk Manager
Common language	That simple and common terms and language is used so that everyone is clear on how this works and what is required of them
Decision making	That there is a direct link between risk and decision making – i.e that a good understanding of uncertainty (risks presenting opportunities and threats) is explicitly considered as part of decision making and resource allocation
Integration with planning	That uncertainty, risk, opportunity, threat, resilience and control, are explicitly addressed as part of the planning process
Integration with operations	That a good understanding of risk/uncertainty, and how this is managed (controls), is embedded into day-to-day operations so that risk management becomes just management

Operating cadence	That the pace of activities is aligned and built into core planning, management, governance and reporting cycles
Performance and monitoring	That core management reporting, monitoring and oversight mechanisms show an integrated picture of commitment, activity, performance, risk and assurance – i.e., what is expected is delivered

Definitions

For the purposes of this policy, the following words are defined to mean:

- ***Risk management:*** The process of enabling relevant information on uncertainty about the future to feed into decision making
- ***Uncertainty:*** Imperfect or unknown information about the future – both in terms of something that could go wrong (threat) or something that needs to go right (opportunity). Those areas of uncertainty that are relevant (i.e. what we care about) are those that affect the ability of HBRC to be successful

7. ***Risk:*** For the purposes of this policy, the terms 'risk' and 'uncertainty' will be used interchangeably and mean the same thing
8. ***Material risk***: an area of uncertainty/risk that, should it occur, should significantly impact on the ability of HBRC to deliver on it's commitments as outlined in its accountability documents – i.e. the Long Term Plan and Annual Plan

- ***Threat:*** The downside of uncertainty – things that could go wrong
- ***Opportunity:*** The upside of uncertainty – thing that could go right
- ***Cause:*** the origin or trigger of a risk – the underlying conditions or areas of uncertainty that might lead to the specific uncertainty/risk being considered
- ***Consequence:*** the outcome or impact that results should the area of uncertainty/risk being considered eventuate (i.e. the 'so what' from this risk)
- ***Decision making:*** Determining what should happen to prevent the risk from occurring and to ensure opportunities are captured (i.e. what controls will be put in place) and allocated appropriate resources (people, money, assets) to achieve this
- ***Control:*** Activities that ensure things go right (or don't go wrong)

9. ***Risk Appetite:*** The level of uncertainty (or variability in performance/outcomes) that is acceptable in order to deliver on HBRC mandate and strategic objectives. In effect a risk will be outside of HBRC's risk appetite when they are rated red or amber per the Risk Management Framework

Risk identification

HBRC wide strategic risks will be identified and documented using a consistent '***One Page Management Plan'*** approach. This provides a consistent basis to define and assess risks in terms of 'uncertainty' presenting both upside opportunity as well as downside threats to HBRC.

Business unit or function specific operational and project risks can be identified using either the same One Page Management Plan approach or more traditional risk register based systems.

Specific templates for these One Page Management Plans enable staff to identify, assess and evaluate risks in a consistent manner across the organisation. These plans require the following factors to be considered:

Area of the One Page Management Plan	Purpose
Focus (i.e. risk / uncertainty)	The definition as to what this risk (area of success or uncertainty) represents. Also identified those accountable for 1) bringing a view of this to the ELT for decision making and 2) ensuring management activities and controls are sufficient
Causes	Each cause represents a specific driver or contributing factor to the central area of success or uncertainty (i.e. risk) – essentially 'sub-risks'. The rating for each cause represents the views of those accountable for this area as to their level of confidence/concern with respect to this area. Each of these causes may then described within it's own One Page Management Plan
Consequences	Describes the consequences of this area of uncertainty / risk – i.e. if well managed, the specific opportunities that might result, or if not the threats that exist that could cause issues for the HBRC
Controls	Controls summarise the major management practices, initiatives, controls, treatments, mitigations in place that collectively address the causes/contributory factors to this area of risks
Assurance	Mechanisms in place to ensure that effective controls are in place and that these are working as expected
Monitoring	Specific outcomes and measures associated with this area of success/uncertainty and the escalation point, that provides the ability to determine whether this area of uncertainty/risk is outside of agreed 'appetite' and whether things are improving or degrading
Gaps	Highlights any significant gaps in activities or controls that manage this area
Response	Based on everything within this page, the response section describes future actions to be taken to address causes/contributing factors and strengthen management controls and monitoring measures

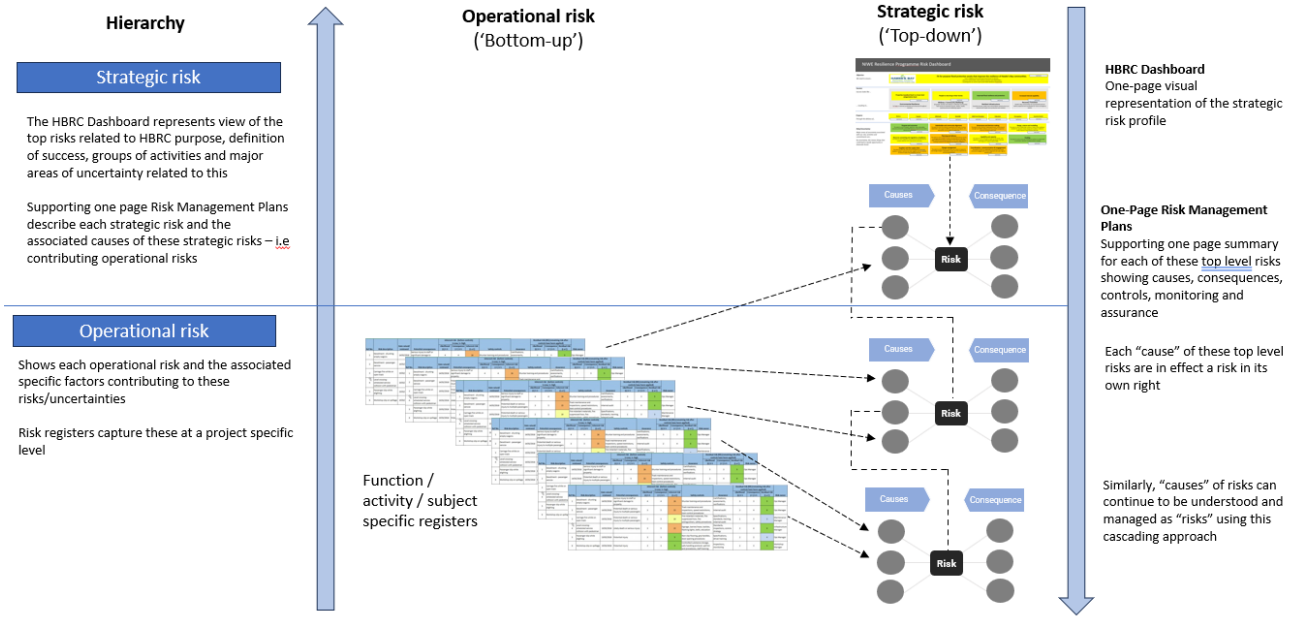
Risk analysis

The purpose of risk analysis is to determine how important this area of risk/uncertainty is to HBRC and the extent to which it is within or outside of agreed threshold (risk appetite).

Two approaches are provided for:

1. **Top down strategic risk**: a rating based on relative ***confidence or concern***
2. **Bottom up operational/project risk**: a rating based on consideration of ***likelihood and impact***

The relationship between a top-down and bottom-up approach to risk management is illustrated below



Appendix 2 provides guidance for analysing top down strategic risk.
Appendix 3 provides guidance for analysing bottom up operational and project risks

Risk treatment

There are five ways that risks/uncertainties can be addressed, which is through a combination of one or more of the following:

Avoid	Eliminate the areas of risk/uncertainty by not engaging in the activity, function or project that this risk/uncertainty relates to
Reduce	Take active steps to reduce the likelihood of this risk occurring and/or the impact on HBRC should it occur
Transfer/share	Pass on to a third party (outside of HBRC) some or all of the consequences of the risk (for example through insurance or outsourcing)
Accept/retain	Live with the likelihood and consequences of this area of risk/uncertainty
Exploit	Actively look to take advantage of this area of risk/uncertainty, and the potential opportunities that this presents.

Risk monitoring, review, reporting and decision-making

For the top down strategic risk approach, a Risk Sentiment Survey is to be completed monthly by the Executive Leadership Team and quarterly by Councillors. The purpose of this survey is to assess the relative level of confidence or concern on each of the areas of uncertainty/risk described within HBRC's strategic risk profile.
This allows:

1. The collective view of the Executive and Councillors to be determined
2. The degree of alignment or divergence of views across this group be determined
3. Areas of heightened concern to be escalated and discussed at ELT and/or Council

The HBRC dashboard (strategic risk profile) is to be provided monthly to the ELT and quarterly to the Risk and Audit Committee of Council.

For the bottom up operational/project risk approach, those accountable for specific risks should confirm that description of these risks (including causes, consequences, controls and risk ratings) remain current and relevant within the risk registers/risk management tools (for example TechOne PLM) they use.

Ultimately, all staff, managers and elected members have accountability for ensuring that material risks they are aware of are documented, described and managed effectively, and reported/escalated appropriately so that this explicitly supports good decision making – i.e. that the following questions are addressed:

- What might happen that could materially impact on HBRC?
- Can we live with this or if not, how are we managing this?
- Is this sufficient and effective?
- If not, what will we do about this?

In short, risk management is central to good management and decision making.

Appendix 2: Risk assessment guidance for strategic risks

Rating	What this means in terms of risk	...or in terms of uncertainty	... and in terms of opportunity	Risk appetite
Red	**Extreme risk** Very significant potential impact on HBRC's operations, people, rightsholders and wider stakeholder trust and confidence Current management practices (controls/mitigations) insufficient to reduce potential exposure to an acceptable level	**Extreme volatility** Very uncertain or changeable environment, that presents major downside (threats) or upside (opportunities) Insufficient or ineffective mechanisms to monitor or respond appropriately to the threats or opportunities that may present themselves	**Extreme opportunity** Very significant areas of opportunity or potential for positive change Current plans, initiative or projects do not fully capture these opportunities and significant gaps exist between what we want to achieve and what we are currently doing to achieve this	***Outside** of 'risk appetite' so action required to manage this to a level that we are comfortable to live with*
	Fundamental concerns, cannot live with this, intervention required as a matter of priority			
Amber	**High risk** Relatively high level of exposure or impact to HBRC Some controls or mitigations in place however these may not be sufficient to reduce exposure to an acceptable level	**High volatility** Quite a changeable environment with respect to areas of major priority or commitment to your organisation A lower level of ability to respond quickly than is desirable	**High opportunity** A relatively high level of opportunity or potential to do things differently Some initiatives in place but may not be sufficient to deliver on our commitments or achieve our strategic priorities	
	Significant concerns, uncomfortable to live with this and we need to do something different			
Yellow	**Moderate risk** A reasonable level of risk faced by HBRC but with a level that your are able to respond to Some controls in place, but could do more or uncertain as to the effectiveness of these controls in practice May cause some pain or disruption, potentially could mitigate further, but broadly in line with risk appetite	**Moderate volatility** Some level of uncertainty or variability faced Reasonable mechanisms to identify and respond to threats or opportunities, should they present themselves	**Moderate opportunity** A reasonable level of opportunity to do things better, more consistently and effectively Some controls in place, but scope to strengthen, enhance and improve these Reasonable opportunity to increase the level of assurance that what we expect to occur is in place and working effectively	***Within** our 'risk appetite', i.e we think we are doing enough at this stage and can live with any residual uncertainty (risk)*
	Some concerns, can live with this currently but would like to do more			
Green	**Low risk** Relatively low level of exposure, but not necessarily no risk Confidence that effective management practices and controls in place	**Low volatility** Highly stable or predictable, little impact on your mandate, commitments or priorities Effective mechanisms identify and respond to change	**Low opportunity** Major areas of opportunity have been captured Little areas of major improvement or potential for positive change Effective initiatives in place to deliver on commitments	
	Reasonably well placed, comfortable to live with this			

Appendix 3: Risk assessment guidance for operational / project risks

Waka Kotaki's Z44 Risk Management Guidance provides a useful basis for assessing operational and major project related risks, particularly because this enables explicit consideration of both upside opportunities as well as downside threats.

		Threat					Opportunity						
		Insignificant	Minor	Moderate	Severe	Extreme	Extreme	Severe	Moderate	Minor	Insignificant		
Likelihood	Almost Certain	LOW	MEDIUM	HIGH	CRITICAL	CRITICAL	CRITICAL	CRITICAL	HIGH	MEDIUM	LOW	Almost Certain	Likelihood
	Likely	LOW	MEDIUM	HIGH	CRITICAL	CRITICAL	CRITICAL	CRITICAL	HIGH	MEDIUM	LOW	Likely	
	Possible	LOW	MEDIUM	MEDIUM	HIGH	CRITICAL	CRITICAL	HIGH	MEDIUM	MEDIUM	LOW	Possible	
	Unlikely	LOW	LOW	MEDIUM	MEDIUM	HIGH	HIGH	MEDIUM	MEDIUM	LOW	LOW	Unlikely	
	Rare	LOW	LOW	LOW	LOW	HIGH	HIGH	LOW	LOW	LOW	LOW	Rare	
		Insignificant	Minor	Moderate	Severe	Extreme	Extreme	Severe	Moderate	Minor	Insignificant		
		Consequence											

Threat likelihood:

	Rare	Unlikely	Possible	Likely	Almost Certain
Likelihood (applicable to Capital Projects)	≤5%	>5% - 30%	>30% - 55%	>55% - 85%	>85%
Frequency (applicable to M&O contracts)	Less than once in 10 years	At least once in a period of >6 - 10 years	At least once in a period of >2 - 6 years	At least once in a period of >1 - 2 years	At least once in a period of 12 months

Opportunity likelihood:

	Rare	Unlikely	Possible	Likely	Almost Certain
Likelihood (applicable to Capital Projects)	≤5%	>5% - 15%	>15% - 25%	>25% - 35%	>35%
Frequency (applicable to M&O contracts)	Less than once in 20 years	At least once in a period of >16 - 20 years	At least once in a period of >10 - 16 years	At least once in a period of >5 - 10 years	At least once in a period of 5 years

Threat consequences:

Rating Scale	Reputation			Performance			
	Stakeholders	Public / Media	Legal/Compliance	Delivery	Cost	Health & Safety	Environmental
Extreme	Disruption to stakeholder relationship slowing progression of nationallystrategic activity, and/or.... Loss of route availability of a national strategic high volume highway	Sustained national and/or international media coverage Intervention by Minister required, possibly leading to loss of Ministerial confidence. Commission of Inquiry instigated	High profile prosecution(s) with potential for custodial sentence	Programme slippage resulting in late delivery by more than 0 days	Negative financial impact of more than $0M.	Loss of life, permanent disability or injury, or multiple serious injuries.	Permanent pollution damage or other environmental damage
Severe	Disruption to stakeholder relationship slowing progression of regionally strategic activity, and/or Loss of route availability of a national strategic highway	Sustained media coverage (weeks) Possible Ministerial inquiry leading to loss of Ministerial confidence/form al enquiry by OAG or statutory agency	Individual prosecution	Programme slippage resulting in late delivery by between 0 and 0 days	Negative financial impact between $0M to $0M.	Serious injury (injuries) requiring specialist medical treatment or lost time greater than three weeks	Significant and widespread pollution or other environmental damage, with long term effects
Moderate	Disruption to stakeholder relationship slowing progression of regional activity, and/or Loss of route availability of a regional strategic highway	Short term (days) media coverage Parliamentary/Minis terial questions or 3rd party investigation	Breach with legal rebuke/ abatement notice/ restrictions	Programme slippage resulting in late delivery by between 0 and 0 days	Negative financial impact between $0M to $0M.	Injury requiring medical treatment or lost time of 1 day to three weeks	Pollution or other environmental damage at a localised level, with medium term effects
Minor	Disruption to stakeholder relationship slowing progression of site specific activity, and/or Loss of route availability of a regional connector highway	Local media coverage for 1-5 days Official information request. Negative feedback from Minister	Breach with letter from authority requesting action	Programme slippage resulting in late delivery by between 0 and 0 days	Negative financial impact between $0M to $0M	Injury requiring short term medical treatment and workplace absence less than one day	Minimum pollution or other environmental damage. Short term effects only
Insignificant	Disruption to stakeholder relationship, and/or Loss of route availability of a regional distributor highway	Local media coverage for 1 day	Breach managed at a regional level	Programme slippage resulting in late delivery by less than 0 days	Negative financial impact of less than $0M	Injury requiring short-term first-aid care and no absence from the workplace	Small scale pollution or other environmental damage is localised with no resultant effects. Contained locally

Opportunity consequence:

Rating Scale	Reputation		Performance			
	Stakeholders	Public / Media	Delivery	Cost	Health & Safety	Environmental
Extreme	Enhancement to stakeholder relationship likely to lead to improved implementation of either national or regional strategic activity, and/or… Improvement of route availability of either a national strategic high volume highway or a national strategic highway.	Enhancement to NZTA reputation from positive international or national media coverage likely to lead to recognition from Minister.	Programme advancement resulting in early delivery by more than 0 days.	Positive financial impact of more than $0M.	Demonstrate Health & Safety innovation likely to lead to changes in international standards.	Demonstrate environmental innovation likely to lead to changes in international standards.
Severe	Enhancement to stakeholder relationship likely to lead to improved implementation of a regional activity, and/or… Potential for improvement of route availability of a regional strategic highway.	Enhancement to NZTA reputation from positive international or national media coverage likely to lead to recognition from NZTA Board.	Programme advancement resulting in early delivery by between 0 and 0 days.	Positive financial benefit between $0M to $0M.	Demonstrate Health & Safety innovation likely to lead to changes in national standards.	Demonstrate environmental innovation likely to lead to changes in national standards.
Moderate	Enhancement to NZTA reputation from recorded regional stakeholder feedback, and/or… Potential for improvement of route availability of a regional connector highway.	Enhancement to NZTA reputation from regional media coverage likely to lead to recognition from Senior Leadership Team.	Programme advancement resulting in early delivery by between 0 and 0 days.	Positive financial benefit between $0M to $0M.	Demonstrate a number of enhancements to Health & Safety best practice.	Demonstrate a number of enhancements to environmental best practice.
Minor	Perceived enhancement to NZTA reputation from non-recorded regional stakeholder feedback , and/or… Improvement of route availability of a regional distributor highway.	Enhancement to NZTA reputation from positive industry media coverage.	Programme advancement resulting in early delivery by between 0 and 0 days.	Positive financial benefit between $ 0M to $0M.	Demonstrate industry leading application of Health & Safety best practice.	Demonstrate industry leading application of environmental best practice.
Insignificant	Perceived enhancement to NZTA reputation from non-recorded supplier/partner feedback.	Perceived enhancement to NZTA reputation arising from an absence of negative media coverage.	Programme advancement resulting in early delivery by less than 0 days.	Positive financial benefit of less than $0M.	Demonstrates compliance with Health & Safety practice.	Demonstrates compliance with environmental practice.

Summary of key document changes and version control				
Version	**Date**	**Key changes to be communicated to staff**	**Document owner**	**Approver**
1.0	07/03/24	Full policy review and upload into the Controlled Document System. Endorsed by RAC at the meeting on 15 February 2024.	Risk & Corporate Compliance Manager	Group Manager Corporate Services
2.0	30/4/25	Full rewrite to align with reset of HBRC's risk management approach	Risk Advisor	Group Manager Corporate Services

POLICY

Title:	HBRC GenAI Policy
Policy number:	CD0056

Team policy owned by:	Information and Communication Technology	**Version number:**	2
Document owner:	Pip O'Connor	**Date policy last reviewed and published:**	2024/10/29
Document approver:	Susie Young	**Next review due:**	2026/10/29

Purpose

This policy is designed to ensure that the use of Generative AI (GenAI) tools such as ChatGPT and Copilot for HBRC business purposes is ethical, lawful, and in compliance with all applicable legislation and Council policies. The policy also outlines different guidelines for the use of open or public AI vis a vis enterprise AI.

This policy has been adapted from the 2023 ALGIM Generative AI Corporate Policy.

Target audience

This policy applies to all employees, contractors, Councillors, temporary staff, and third parties with access to GenAI tools, whether they are enterprise GenAI tools or open AI, in pursuit of Council activities.

The scope excludes the use of other LLM (Large Language Models) or machine learning models that may be inherent in software and industry applications. It is limited to interactive GenAI tools.

Policy details

1. **Governance of GenAI Use Within HBRC**
   - 1.1. Use of GenAI within HBRC will be governed by the Digital Governance Group, which is chaired by the CIO. A separate Terms of Reference for this Group will be provided.

2. **Authorised Use**
   1. Employees are authorised to use GenAI for legitimate work-related purposes, subject to the conditions within this policy and general acceptable terms of use.
   2. Note: This policy distinguishes between (1) Licensed, Enterprise GenAI and (2) Public or Open-Source GenAI, with different guidelines for each.

3. **Use of Licensed, Enterprise GenAI At HBRC**
   - 3.1. Employees are entitled to use licensed, enterprise-grade GenAI, i.e. GenAI that has been licensed by HBRC, for legitimate business purposes, including with the use with HBRC data.
   - 3.2. Enterprise licenses are allocated by ICT upon approval from the Digital Governance Group and budget approval from the Group Manager. Requests for these licenses can be made to Service Desk.

3.3. Note: As at FY24/25 **the only authorised Enterprise GenAI tool is licensed Microsoft Copilot for M365 (including approved extensions), and publicly available 'Microsoft Copilot' when signed in with an HBRC work account. This may expand over time.**

4. **Use of Public or Open-Source GenAI at HBRC**

4.1. Employees may use public or open-source GenAI tools such as ChatGPT to assist with legitimate HBRC activities, subject to the conditions within this policy.

4.2. However, HBRC **does not endorse** the use of public, or open-source GenAI tools using confidential HBRC data, or if HBRC data will be used to train the generative model.

- This is because the data may enter the public domain and could release non-public information and/or breach regulatory requirements, vendor contracts, or compromise intellectual property.
- Open-source or public AI may also store sensitive data and information, which could be at risk of being breached or hacked.
- See "Data Privacy and Security" section for guidelines on what data can be used with public or open-source GenAI.

4.3. If using Public or Open-Source GenAI tools

- The employee will be responsible for ensuring that the GenAI tool being requested is fit for purpose, and that it will be used in a way that is in accordance with appropriate laws, regulations and adheres to HBRC's internal security and privacy and acceptable use policies.

5. **Data Privacy and Security**

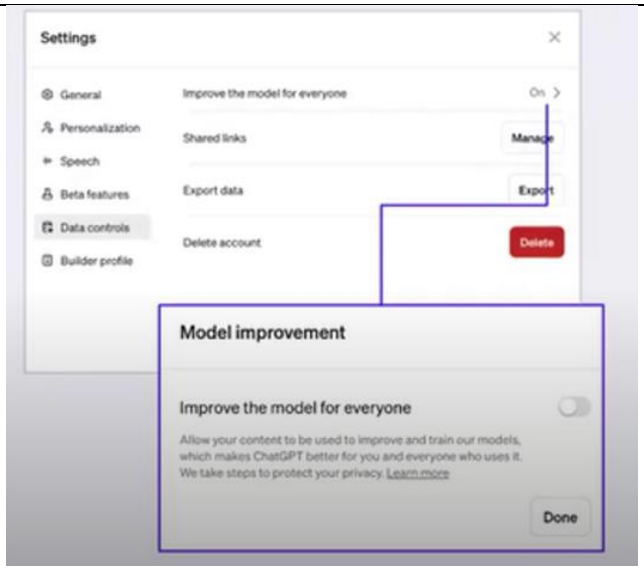
5.1. It is important that we keep our data, including data that we hold about our rate payers, safe. And employees must follow all applicable data privacy laws and organisational policies when using GenAI

5.2. If using a **licensed, enterprise GenAI tool**:

- HBRC data can be used with the model.
- It is recommended that personal information of employees, councillors or rate payers is anonymised before using it in a prompt.

5.3. If an employee is **using public or open-source GenAI technology for business use**, employees must first:

- Ensure that the tool is fit for purpose.
- Review its suitability when considering any privacy, security, reputational, copywrite, bias or data integrity issues that may arise from the use of the GenAI
- Turn off the model's ability to train on the data you provide – for example, with ChatGPT, this can be turned off in the "Settings" (see below)



5.4. Ensure they anonymise any HBRC data that will be used by the model, for example,

- The following framework provides guidance on the types of data that can/cannot be entered into **public or open-source GenAI tools.**

Category	Restriction	Example Data Type
Red	Do not include in any AI prompts with public or open-source AI	• Personal information of employees, councillors or rate payers • Internal confidential data • Confidential business or personal information belonging to third parties e.g. vendors and suppliers
Yellow	OK to use in public and open-source AI prompts, but anonymise to protect sensitive information	• Consultation and survey feedback (anonymised, Personal Identifying Information (PII) must be removed) • General industry research and data
Green	OK to include in public and open-source AI prompts and materials shared with AI	• Any information already available to the public

6. Usage Guidelines

6.1. Accuracy and Accountability

- If an employee generates content with the use of GenAI, the **employee remains accountable for the content**.
- It is the employee's responsibility to ensure the accuracy and appropriateness of the content and should always review and edit responses for accuracy before utilising the content.

6.2. Information Security Breach

- If employees access HBRC information they are not entitled to access using GenAI, this should be reported immediately to their Manager and to the CIO so that the security controls can be remedied.
- Failure to report an information security breach may result in disciplinary action.

6.3. Ethical Use and Bias

- Employees should use GenAI responsibly and ethically, in compliance with Council policies and applicable laws and regulations.
- Employees must not use GenAI to generate content that is discriminatory, offensive, or inappropriate.

6.4. Copyright

- It is prohibited to use GenAI to generate content that infringes upon the intellectual property rights of others, including but not limited to copyrighted material.

6.5. Meeting Recordings and Disclosure

- It must be disclosed to meeting participants when meetings are being recorded or transcribed with AI.
- It is encouraged to identify and disclose content as containing AI-generated information, where this is appropriate.

6.6. LGOIMA

- Any content generated by AI for HBRC business purposes, including meeting transcripts and meeting summaries, can be subject to a LGOIMA request. This content must be treated with the controls as human-generated content e.g. saved in an appropriate place.

7. Use of Alternative, Purchased GenAI Tools

7.1. If an employee wishes to purchase new GenAI technology or licenses for business use, Employees must:

- Obtain approval from the Digital Governance Group, with requests sent in advance to the IT Service Desk.
- Determine whether the GenAI will ingest any HBRC organisation or HBRC personal data, and if so, ensure that this will be stored appropriately, with respect for relevant privacy and access controls.
- ICT may keep a register of any purchased GenAI tool, the people using it, the nominated business owner, the license structure, the vendor, agreed vendor management, and the intent behind the tool.

8. Licenses and Support

8.1. ICT will only manage the licenses and vendors for approved Enterprise GenAI tools.

8.2. ICT will only provide technical support for approved Enterprise GenAI tools

8.3. Funding for Enterprise GenAI tools will be decided by ELT and the Digital Governance Group

9. **Use of Extensions, Connectors, APIs and Plugin tools for GenAI**

9.1. 3rd party connectors and extensions (including the use of Copilot Studio and the development of new bots) that extend authorised Enterprise GenAI can be created and used, in line with these policy guidelines.

9.2. Custom-built extensions and plugins can be developed for legitimate business purposes.

9.3. The intent to publish or deploy any AI extensions, connectors, APIs or plugins (etc) must be notified to ICT in advance, via the Service Desk.

9.4. A register may be kept for purposes such as reuse, support and/or extendibility.

9.5. ICT reserves the right to refuse the permission for new AI tools, connectors, plug-ins, APIs, extensions etc, if they do not meet ICT standards, including but not limited to security and infrastructure compliance.

9.6. Funding for Enterprise GenAI tools will be decided by ELT and the Digital Governance Group

Policy Compliance

10. Any violations of this policy should be reported to the CIO or the Digital Governance Group.
11. Failure to comply with this policy may result in disciplinary action.

Policy Review

12. This policy will be reviewed twice per year at a minimum, and updated as necessary to ensure continued relevance, and compliance with all applicable legislation, regulations, and organisational policies.

Acknowledgement

13. Employees acknowledge that they have read and understood this policy, including the risks associated with the use of GenAI.
14. Employees also agree to comply with this policy and to report any violations or concerns to ICT.

Summary of key document changes and version control

Version	Date	Key changes to be communicated to staff	Document owner	Approver
01	23/10/2024	First Version	Pip O'Connor	Susie Young
02	29/10/2024	Updated with information from IA course	Pip O'Connor	Susie Young

Policy

Title:	ICT Acceptable Use Policy
Policy number:	CD0002

Team policy owned by:	Information and Communication Technology	**Version number:**	5
Document owner:	Kaylie Hammond	**Date policy last reviewed and published:**	2025/08/11
Document approver:	Pip O'Connor	**Next review due:**	2026/08/11

Purpose

The purpose of this policy is to outline what is acceptable use of Hawkes Bay Regional Council's (HBRC) information systems and devices. The policy aims to ensure that all users maintain safe, ethical effective use of HBRC Information systems and devices and comply with legal requirements. It is the responsibility of every user of HBRC information systems and mobile devices to know these guidelines and to abide by them.

Target audience

This policy applies to all staff (including contractors, Councillors, casual staff, and students) that utilise HBRC information systems. All are required to read, understand, and agree to abide by this policy.

Policy details

1. **Policy goal or objective**

1.1. The goal of this policy is to ensure that HBRC's information/data assets, software and systems are protected from intentional and unintentional threats when used. The policy aims to ensure the:

- Safe operation of applications and software implemented on HBRC's IT (Information Technology) systems.
- Information/data HBRC collects and uses has integrity, is legally compliant, is available, and upholds HBRC's values (ethical).

  - Related documents
  - Information Management Policy
  - Employee Policy Handbook
  - Social Media Policy
  - Procurement Policy
  - Motor Vehicle Use and Safe Driving Policy
  - Privacy Policy
  - Internal Fraud Policy
  - ICT Hardware Policy
  - ICT Administrator Access Policy
  - HBRC Generative AI Policy

2. **Key definitions/abbreviations**

- **Information system**: all HBRC owned and managed devices and equipment used for the collecting, storing, and processing of data and communications. This includes HBRC's IT systems, network, software, and hardware.
- **Mobile device:** includes a mobile phone, smart phone, tablet, radio transmitter (RT) or any mobile data device.
- **Users:** anyone that is contracted by HBRC and requires access to HBRC information system, network, and applications
- **ICT:** Information Communication & Technology

3. **Access Control**

3.1. Permission to access information is granted to each user based on their role requirements and the business needs of HBRC. These permissions are approved by the relevant Group Manager.

3.2. The connection of devices such as portable computers, laptops, mobile devices and iPad's to HBRC's corporate network must be approved by the Information, Communication and Technology Team (ICT). ICT will ensure the appropriate access controls are installed. This is to ensure that HBRC can control the risk of security threats and manage the boundaries of HBRC information systems.

4. **General Use and Ownership**

4.1. HBRC is required to protect its network and comply with the Privacy Act 2020, therefore:

4.2. Any data that users create on HBRC's information systems and mobile devices remains the property of HBRC.

- ICT may monitor equipment, systems, usage, and network traffic at any time.
- Users must complete all mandated information system security training.

5. **Personal Use of Hawkes Bay Regional Council Information Systems**

5.1. Personal use of HBRC information systems is allowed providing it is 'reasonable' and 'appropriate' and does not impact on staff productivity. It is important that users are aware for reasons outlined in Section 4 'General Use and Ownership.' HBRC does not guarantee the confidentiality or security of any personal information stored on any network device that belongs to HBRC.

5.2. The personal use will be deemed as 'unreasonable' if it:

- Adversely impacts on the performance of normal job responsibilities.
- Precludes other users from accessing the device or information systems.
- Adversely impacts on the performance or stability of HBRC's information systems or Internet connection e.g., downloading of large files, or using the Internet for personal entertainment.
- It is during normal working hours, other than users permitted breaks.
- Breaches the ICT Acceptable Use Policy

5.3. While HBRC respects its employees right to privacy, employees that use HBRC's information systems, HBRC's internet connection, or any HBRC mobile devices have agreed that:

- All use is monitored as guided by HBRC's network administration procedures and protocols.
- Use and access complies with HBRC policies and all legal obligations.

5.4. HBRC information systems and mobile devices must not be used to conduct personal commercial activities.

6. **Account and Password Security**

6.1. User IDs, passwords, PINs, door swipe cards, or other forms of identity must not be disclosed to anyone, shared with anyone or written down.

6.2. Network system users will be prompted to change their password every 365 days. Strong passwords are required that must be at least 14 characters in length and contain three of the following: upper- or lower-case letters, numbers, or special characters.

6.3. All users must use Multi factor authentication (MFA) to access their accounts.

6.4. Group or generic User IDs and passwords are prohibited as a rule, but in special circumstances may be approved by the HBRC's Chief Information Officer (CIO)

6.5. All contractors or other third parties' access to HBRC information systems must be approved by the relevant Group Manager and IT Service Desk. The contractor will be issued with a unique login which will be removed or shall expire once the work has completed.

7. **Security of information**

7.1. Any information or data created, manipulated, saved, transmitted, or archived using HBRC owned or managed information systems or mobile devices, remains the legal property of HBRC.

7.2. Any information or data created while employed or on contract to HBRC is deemed to be HBRC owned intellectual property and cannot be used, shared, or sold without approval.

7.3. Electronic files must be accessed, used, and stored in accordance with their classification as defined by the HBRC, 'Information Management Policy.' Data should be saved to a network drive or online. IT Service Desk can be contacted to provide guidance.

7.4. All information whether in soft or hard copy held by HBRC on any network, device or in any physical location is subject to the provisions of Privacy Act 2020. All users and employees must familiarise themselves with HBRC's Privacy Policy and obligations relating to personal information under the Privacy Act.

7.5. Any confidential information belonging to HBRC, must not be disclosed except as expressly permitted under HBRC policies or as required by law e.g., under Privacy Act or Local Government Official Information and Meetings Act (LGOIMA). This includes disclosure using email, internet, social media, bulletin boards, list servers or printing, photocopying and/or distributing a physical document.

7.6. From time-to-time users may be required to sign a confidentiality or non-disclosure agreement. It is important when a non-disclosure agreement is in place that information is to be classified as follows:

- Not to be stored - information which may not be captured or saved in electronic systems.
- Confidential - information restricted to a small number of people.

- Internal Use Only - information which may be known by staff, but not by anyone external to the HBRC.
- Public - information that is approved for public dissemination.

7.7. Removable media or storage devices, such as CDs, DVDs, or USB are susceptible to loss or theft. Use of personal removable media or storage devices are prohibited. If these are required, Service Desk have approved removable media forms and information held on removable media must be classified and handled appropriately.

8. **Security Incidents**

8.1. Users of all HBRC owned and managed devices, information systems and networks must notify management as soon as possible of any condition that could lead to a disruption of normal business activities. These include but are not limited to:

- Ineffective security controls
- Issues relating to information integrity, confidentiality, or availability
- Human error
- Non-compliance with policies or guidelines
- Breaches of physical security arrangements
- Uncontrolled system changes
- Access violations
- Missing or stolen equipment
- Weaknesses in security or potential security vulnerabilities
- System malfunctions
- Missing files
- Potential hazards in the workplace such as electrical wiring hazards
- Malware/virus or Phishing incidents

8.2. The ICT department reserves the right to implement new, or change existing, security protocols as needed to ensure the safety of the HBRC network and devices.

9. **Modification of Software and Hardware configurations**

9.1. Users are not permitted to install new or modify existing software or hardware configurations on the HBRC network or mobile devices without the approval of the IT Service Desk. This includes:

- Changing operating systems settings
- Changing application settings (including the location of software and files)
- Installing or removing software, including applications downloaded from the Internet
- Disabling virus protection
- Adding or removing users
- Changing user privileges
- Adding, removing, or modifying computer hardware
- Changing configuration of enterprise systems without going through the appropriate change approval process.

10. **New Software, Applications, AI, Servers, Networks**

10.1. All requests to purchase and/or develop new technology, including but not limited to software, applications, AI, servers, networks, plugs etc must be referred to the IT Service Desk for assessment and approval before proceeding.

10.2. Purchase requests must also abide by the requirements detailed in the HBRC Procurement Policy.

11. Mobiles Devices

11.1. Users of mobile devices:

- Must comply with the rules under Section 12 'Prohibited Use'.
- May onboard their own number where appropriate e.g., not a duty phone
- Can use their own mobile device, if preferred, however HBRC will:
  - Not pay for any plan cancellations or device repairs if broken when being used for business purposes.
  - Not be responsible for anything personal stored on the device.
  - Install mobile device management and enforce a PIN control. When a staff member leaves, they must have IT remove the corporate applications.
  - Wipe the phone if it is lost to safeguard HBRC data. Therefore, the individual is responsible for backing up any personal data/ photos / information.
- Can use HBRC mobile plans issued for HBRC business purposes for reasonable and appropriate personal use providing:
  - Reasonable use for calls and text messages in line with the corporate mobile plan, see related documents for further detail.
  - The data plan is not exceeded due to personal use,
  - The personal use does not cause HBRC to incur any additional costs or impact staff productivity.
  - ICT monitors mobile use when on the corporate plan and has the right to query excess data / mobile usage, and remove or change the mobile plan if excessive use is observed.
- Must ensure text messages or other forms of communications are legible, polite, and professional whether HBRC related or under reasonable personal use.
- Must ensure all voice recordings, text messages, photo images or data processed on a mobile device that meet the definition of a formal business 'record' be transferred off the device and stored appropriately within the HBRC's electronic document records management system (eDRMS).
- Will only download applications through approved application stores onto mobile devices e.g., Apple's App Store or Google's Google Play.
- All changes to configuration or maintenance of the device must be carried out by IT Service Desk.
- Must ensure that the device is protected by a PIN number and auto-lock. Voice and bio-metric authentication must be coupled with password or PIN authentication. Mobile devices used to store important HBRC information and users must ensure that this information is protected from unauthorised access.

- Must immediately report to the IT Service Desk or their Team Leader if a mobile device used for HBRC activities is lost, stolen, damaged or unavailable for normal business use.
- When travelling in vehicles, only use a mobile phone to make, receive or terminate a telephone call if the vehicle has stopped for a reason, other than the normal starting and stopping of vehicles in a flow of traffic, unless a suitable hands-free kit is available to receive calls. Refer the Motor Vehicle Use and Safe Driving Policy
- If an employee is going to be leaving the country,
  - They need to get their manager's approval to use the HBRC device outside of New Zealand.
  - When travelling internationally, must inform IT Service Desk to enable roaming if the phone is to be used whilst overseas.
  - If travelling overseas any roaming costs for personal use may be recharged to the user.

11.2. All HBRC allocated mobile devices and any HBRC business information stored on any mobile device it is the property of the HBRC and must be returned at the time the employee leaves or the contract ends. The device and the information stored on it can be inspected or used in any manner and at any time by authorised HBRC staff or their agents.

11.3. HBRC is not responsible for any personal information stored on HBRC issued devices. Information and applications may be removed by HBRC if they are not work related.

11.4. ICT manages the issue, service, and administration of HBRC devices. ICT acts as HBRC's representative with nominated service providers to facilitate the purchase, replacement and repair of equipment and initiate resolution of technical problems. Devices will have mobile device management tools installed to secure data and assist with remote support.

11.5. HBRC maintains the right to conduct inspections and search any device that it owns or manages without prior notice to the user. The device must be returned to the IT Service Desk upon request for maintenance, updates, and when the user ceases to provide services to HBRC.

11.6. International calls and texts (not covered by the corporate plan) should only be work related unless it is a genuine personal emergency, and there is no other way to contact the other party overseas. Any costs incurred relating to the above will be the responsibility of the staff member.

11.7. HBRC may monitor the usage of all HBRC mobile numbers and mobile devices and access all device information, including usage and websites visited.

12. Prohibited Use

12.1. This list below while not exhaustive, provides a framework for types of activities that are deemed unacceptable and therefore prohibited, this should be read in conjunction with HBRC's Social Media Policy. Users may be exempt from certain restrictions due to their job responsibilities e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services.

- General prohibited use and activities:
  - Procuring, creating, storing, displaying, copying, transmitting, or distributing any file or material that is:
    - objectionable

  - copyright protected e.g., digital media, photographs, music, or software not licenced to HBRC etc.
  - in breach of New Zealand law.
- Infringing on the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations.
- Using unauthorised file sharing software or programs.
- Introduction of malicious programs into the network or server e.g., viruses, worms, Trojan horses, e-mail bombs, etc.
- Revealing account passwords or allowing use of the account by others e.g., by family or other household members when work is being done at home.
- Making fraudulent offers of products, items, or services originating from any HBRC account.
- Effecting security breaches or disruptions of network communication, including, but are not limited to:
  - Accessing data of which the employee is not an intended recipient.
  - Logging into a server or account that the employee is not expressly authorised to access.
  - Network sniffing, ping floods, packet spoofing, denial of service, and forged routing of information.
- Providing unauthorised HBRC employee information or lists to outside parties.
- Port scanning or security scanning, unless performed by ICT.
- Executing any form of network monitoring which will intercept data not intended for the employee's host, unless performed by ICT.
- Circumventing user authentication or security of any host, network, or account.
- Interfering with, or denying, service to any user other than the employee's host e.g., denial of service attack.
- Locally or via the Internet /Intranet /Extranet using any program/ script/ command, or messages with the intent to interfere with or disable a user's terminal session.
- Copying software off HBRC Information Systems.
- Copying a file or an email off HBRC Information Systems, unless authorised to do so, or it is a personal file or email.
- Deleting software, a file, or an email from HBRC Information Systems, unless authorised to do so, or it is a personal file or email.
- Deliberately accessing or attempting to access parts of HBRC Information Systems, software, or files which do not require job access.
- Moving any hardware inside the premises, or removing any hardware from the premises, unless expressly authorised to do so by the IT Service Desk.
- Attempting to fix any hardware or software that does not appear to be working properly, or any HBRC Information System security flaw, unless expressly authorised to do so by the IT Service Desk. Hardware or software failure or security flaw should be immediately reported to the IT Service Desk

- Sending or forwarding unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
- Harassment whether through language, frequency, or size of messages.
- Facilitating unauthorised or fraudulent use, including sending anonymous emails or emails which appear to the recipient to have been sent by someone other than the sender.
- Posting non-business-related messages to large numbers of newsgroups (spam)
- Representing yourself as not who you are.

- Internet prohibited use and activities:
  - Representing yourself as not who you are on the Internet.
  - Using the Internet to search, transmit confidential, political, obscene, threatening, or harassing materials.
  - Downloading or accessing any material of a pornographic, racist, or extreme political nature, or which incites violence, hatred or any illegal activity is strictly prohibited. Many sources or destination addresses that contain such material are blocked automatically notify IT Service Desk immediately of anyone trying to access such addresses.
  - Downloading and installing software from the Internet onto the HBRC devices. If there is an absolute business need IT Service Desk must be contact.
  - Downloading non-work-related material from the Internet.
  - On-line gambling or any other illegal activity within New Zealand or the country of receipt.
  - Using the Internet to access (or attempt to access) another computer, or files on another computer, that users are not authorised to access (or intended to be able to access) by the owner of that computer.
  - Using VPN or reverse proxy activities to stream unlicensed content e.g., Movies.
  - Bypassing corporate security by any means.
- Mobile Devices prohibited use and activities:
  - Mobile devices supplied by HBRC must not be altered or added to in any way including:
    - unauthorised upgrades
    - addition of components
    - removal of components - including transferring a HBRC SIM card to a personal phone
    - altering configuration or security settings
    - jailbreaking the device
  - Mobile devices apps must not be downloaded if they compromise the safety and security of the device, or breach copyright law.
  - Mobile devices allocated to users for business activities must not be lent to others external to HBRC, including friends and family.

- Devices on HBRC's corporate plan must not be used for charged services such as:
  - "Text to Park" - if an employee needs to pay for parking, use cash or a credit card and claim it back if its business related.
  - "Entering competitions or donating to a cause - HBRC does not pay these personal costs. If these charges are incurred the user will be invoiced by Finance.

13. **Breach of policy – consequences of non-compliance**

13.1. Failure to comply with this policy may be considered potential misconduct or serious misconduct and as such may result in disciplinary action, up to and including termination from employment".

14. **Related Documents**

14.1. Corporate Mobile Plan

Summary of key document changes and version control				
Version	**Date**	**Key changes to be communicated to staff**	**Document owner**	**Approver**
1	08/08/2023	Full review of previous Acceptable Use Policy (maintained outside of the system) and Upload into HBRC controlled document system.	Team Leader ICT Infrastructure and Support – Jen Ellingham	Group Manager Corporate Services – Susie Young
2	30/09/2024	Full review of previous Acceptable Use Policy and Upload into the HBRC controlled document system	CIO – Pip O'Connor	Group Manager Corporate Services – Susie Young
3	14/02/2025	Added in a link to the corporate mobile plan	Business Support Team lead – Kaylie Hammond	CIO – Pip O'Connor
4	28/05/2025	Added further info on breaches and failure to comply statement	Business Support Team lead – Kaylie Hammond	CIO – Pip O'Connor
5	11/08/2025	Update password policy under section 6	Business Support Team lead – Kaylie Hammond	CIO – Pip O'Connor