Policy on Dealing with Malicious Communication

(Staff Related)

Author	Director of IT
Date	March 2025
Person Responsible	Executive Director of Facilities and Resources
Approval/ review body	SLT
Frequency of Review*	36 months

** Policies will be reviewed more frequently if legal changes or good practice require*

Review History:		
Date	Reviewed by	Reason for review
Jun 2012	IT Director	General update to include staff
Oct 2015	Executive Director of Facilities & Resources	Review
Apr 2019	Executive Director of Facilities & Resources	Review
Mar 2024	Deputy Executive Principal, Teaching, Learning and Improvement	Update to include situations of in person abusive communication and remove references to learners.

Contents

Related policies/documents:

1. Mobile Device and Communication Policy
2. Information Technology Conditions of Use Policy
3. Data Breach Policy and Procedure
4. Behaviour Policy
5. Prevent Policy
6. Safeguarding Policy.

NOTE – This Policy, together with the Policies and Procedures listed above, seek to ensure, so far as reasonably practicable, that the College is fulfilling its duty under sections 26 and 29 of the Counter-Terrorism and Security Act 2015 and the Prevent Duty (2023). The College will participate fully in work to prevent people from being radicalised or drawn into extremism and, will ensure that, should this occur, there are procedures in place to deal with them.

1. Statement

North Kent College, which incorporates Hadlow College, hereinafter referred to as "The College" is aware that malicious communication may enter the organisation via various routes and recognises such communication may not only cause distress to the person or persons who may be the subject but may also be an early indication of a more serious situation. Malicious communication may originate from inside the organisation or externally and may bring the College into disrepute.

For the purposes of this Policy, it will largely focus on communications with staff, with the understanding that any malicious communications received or sent by the College's learners would be dealt with under the College's Behaviour Policy.

2. Objectives

The objectives of this policy are to:

2.1. identify the source of malicious communication as early as possible, so that appropriate action can be taken to prevent further distress or harm;

2.2. assess the potential risk to the health, safety or welfare of staff, or visitors;

2.3. assess the reputational risk of the College; and

2.4. provide support or protection as necessary to the subject of any malicious communication or anyone else identified as being at risk.

3. Definitions

Malicious Communication:	Any communication of a defamatory, bullying, threatening, harassing, or offensive nature, received by the organisation's staff or visitors in the course of their employment or involvement with the College. It may be made in person or arrive by post, e-mail, phone or any other means.
Visitor:	Anyone who is not a learner, or member of staff.
Harm:	Loss of or damage to a person's rights, property, or physical or mental well-being.

4. Types of Communication

In the modern world, communication can take place using a number of methods including electronic and traditional means whether received in person or online:

4.1. Verbal;

4.2. Written;

4.3. Photocopied (Printed);

4.4. Telephonic;

4.5. Email, SMS and Instant Messaging (text, attachments/links to image(s)/video/audio);

4.6. Social Network and blogging; and/or

4.7. Mobile telephone and other electronic devices.

5. Responsibilities

5.1. Chief Executive and Executive Principal

5.1.1. make resources available for the operation of this policy; and

5.1.2. ensure that concerns raised by visitors, or staff relating to malicious communication are brought to the attention of the Deputy Chief Executive.

5.2. Deputy Chief Executive

5.2.1. decide on the level and nature of the risk posed by any malicious communication to staff;

5.2.2. attempt to identify the source of such communication. Advice may be required from the IT Department, in the case of electronic communications received via the organisation's IT systems;

5.2.3. take necessary action as quickly as possible to deter further malicious communications from that source or mitigate the potential harm;

5.2.4. involve the police, where necessary; and/or

5.2.5. recommend disciplinary action where appropriate through the People Department.

5.3. Data Protection Officer ("DPO")

5.3.1. maintain a Central Record of Malicious Communications to staff;

5.3.2. collate related items of malicious communication; and

5.3.3. assist the College in assessing the potential risks posed and advise the Deputy Chief Executive.

5.4. Line Managers

5.4.1. adopt a supportive approach to any member of staff who reports that they are the subject of malicious communication;

5.4.2. arrange for any items of malicious communication related to staff to be forwarded to the DPO.

5.4.3. advise staff who may be the subject of malicious communications and may be experiencing stress or concern as a result, of the support that is available to them through the People Department or Welfare & Safeguarding, respectively.

5.5. Staff

5.5.1. report any malicious communication, however received, to their Line Manager or senior lead; and

5.5.2. be aware of the Online Social Media and Telecommunications Guidelines outlined in the IT Conditions of Use Policy.

5.6. Visitors

5.6.1. report any malicious communication, however received, to the Chief Executive and Executive Principal via the College's online Complaints procedure via the College website.

6. Procedures

A staff member receiving malicious communication from an external source must bring it to the attention of their Line Manager as soon as something is received. If a malicious communication is received by a staff member from an internal staff member, then this may need to be reported directly to the People Department. If any communication alleges a direct and immediate threat to the health of any individual, immediately inform as appropriate Security, or to the most senior manager present at any of the College campuses.

6.1. Communications Received by Phone

This section outlines the various scenarios relating to telephonic communications.

6.1.1. Angry/Abusive Caller linked to an enrolled learner

Where a caller is becoming upset or annoyed and begins to use threatening, crude or abusive language to a member of staff, the member of staff will calmly ask the caller to moderate their tone and/or language.

If the caller persists in using this type of language, the member of staff will repeat the request for the caller to moderate their tone and/or language and advise that should the caller not adhere to this request, they will terminate the call.

If the caller persists, the member of staff will advise that they are terminating the call. The staff member should then let their senior lead know about the call, so that the senior lead can pick the matter up and decide what course of action to take moving forward. The senior lead will need to phone or email the caller and explain how the College expects future communications to come into College and who they may or may not contact directly in future.

6.1.2. Threatening Caller (one where it is deemed the health and safety of any member of the college community is at risk) - not linked to an enrolled learner

So far as possible, write down the exact words of the message. Obtain as much information as possible such as:

6.1.2.1. Name, address, telephone number;

6.1.2.2. Does the caller represent an organisation;

6.1.2.3. If the phone displays the caller ID, write down the number;

6.1.2.4. Time, date and duration of the call;

6.1.2.5. The number of the phone on which the call was received;

6.1.2.6. Background noise - traffic, music (call box, pub etc.), voices, laughing; and

6.1.2.7. Speaker's gender and/or sex, approximate age, accent, was he/she rambling, drunk, laughing?

The form in Appendix 1 will be of use in recording these details.

6.2. In Person Communication on North Kent College Premises

6.2.1. Where a member of the public (whether linked to a learner or not), and is not behaving in a polite and calm, non-threatening manner, may be asked to leave the premises. The member of staff or any colleague in the vicinity will contact Security and/or a senior lead on the College campus to assist, where needed.

6.2.2. If the individual refuses to leave, the College may decide to call the Police.

6.3. Communication Received in Written/Printed/Physical Format

Handle the item as little as possible and pass it to your Line Manager or a senior lead on the College campus, who will then place it in a plastic bag or envelope, seal it and forward it to the DPO, attaching a note giving as much detail as possible, such as recipient, route through which it was received and date of receipt.

The DPO will take the matter forward with the Senior Leadership Team. The College retains the right to escalate matters to the Police as necessary.

6.4. Communication Received Electronically

DO NOT DELETE any communication received via electronic means such as emails, SMS (texts), Social Networking and Blogging/Vlogging sites/comments or any other form of electronic communication. For externally sent messages, inform your Line Manager who will support you in forwarding your message to the DPO.

The DPO will take the matter forward with the Senior Leadership Team. The College retains the right to escalate matters to the Police as necessary.

For internally sent and received malicious communications, you may need to share the communication with the People Department if you wish for the matter to be investigated and taken further.

6.4.1 Processing

The College uses sophisticated electronic tools to track both email and web traffic and will use these tools to bring evidence against the perpetrators of malicious communication.

Once notified of a malicious communication, the DPO will check the central record of malicious communications, to identify any possible links with other communications received previously. The Director of IT will decide on the appropriate course of action, based on the best perceived level of risk. Actions may range from, but are not limited to, keeping the communication on file, to full police involvement. The original recipient will be informed of the actions taken.

Staff should be aware that malicious communication sent by them, by any of the means indicated above, could be regarded as gross misconduct by the College and could result in disciplinary action being taken, with possible dismissal.

7. Support

The College takes the welfare of its staff very seriously. If a member of staff has been subjected to abusive and/or threatening behaviour and found this to have affected their

mental health and/or wellbeing, they can use the Counselling service provided free of charge via the College's Employee Assistance Programme, *Wisdom*.

8. Strategies

8.1. If communications are persistent to either an individual or to many staff across the organisation, the college can adopt a 'single point of contact' approach with that individual. Staff may be asked to set up 'forwarding' on their emails so that the designated single point of contact receives the communication if this strategy has been invoked. The designated person will either be a middle manager or senior leader depending on the situation and level of concern the sender has posed.

8.2. If the individual does not adhere to the single point of contact, that individual will be informed in writing that they can only send written communications by post as no member of staff will deal with them electronically or through the telephone.

8.3. If necessary, the senior lead will discuss with the Chief Executive and Executive Principal as to whether we need to seek legal advice and guidance on the matter to alleviate the burden of the malicious communications.

8.4. If a family member or friend related to a learner comes on site without a prior meeting and enters through the external safeguarding barriers designed to prevent external persons gaining access to the site, the College may call the Police if the intruder refuses to leave of their own volition when asked.

8.5. The Senior Leadership Team member will review the situation and decide whether:

8.5.1 the behaviour of the abusive individual was such that they will be banned from all College locations including but not limited to all areas open to the public, car parks and College events;

8.5.2 where an individual has been banned from all College property; they will only be allowed to communicate with the College by written means; telephone; or via a virtual meeting. If this is untenable, they will need to put all communications in writing; and/or

8.6. If a person gains access to the site and makes any kind of threat to staff or learners, the College reserves the right to prioritise the safeguarding of all parties, and may therefore, in extreme circumstances, withdraw a learner linked to said party, if by having the learner as a member of the College community, puts others at risk by association.

Appendix 1 – Telephone Threat Record

This should be completed once the caller has hung up and you have informed Security Reception or the Senior Manager (at any of the College's satellite sites) if the caller made a threat regarding the safety of any individual.

Time and date of the call: _____

Length of the call: _____

Number at which received: _____

About the caller:

Gender of caller: Male ☐ Female ☐ Unsure ☐

Nationality: ..... Age: .....

Threat Language:

Well Spoken ☐ Irrational ☐ Taped ☐ Foul ☐

Incoherent ☐ Message read by threat maker ☐

Caller's Voice:

Calm ☐	Crying ☐	Clearing Throat ☐	Angry ☐
Nasal ☐	Slurred ☐	Excited ☐	Stutter ☐
Disguised ☐	Slow ☐	Lisp ☐	Accent[1] ☐
Rapid ☐	Deep ☐	Familiar[2] ☐	Laughter ☐
Hoarse ☐			

[1] What Accent? .....

[2] If the voice was familiar, whose did it sound like? .....

Background sounds/noises

Street ☐	House ☐	Animal(s) ☐	Crockery ☐
Motor ☐	Clear ☐	Voice ☐	Static ☐
PA System ☐	Booth ☐	Music ☐	
Factory Machinery ☐			Office Machinery ☐

Other (specify) .....

.....

Remarks

.....

.....

.....

Signature: ..... Date: .....

Print Name: .....