Policy on Dealing with Malicious Communication

Author	Sean McCormick, Director of IT
Date	July 2022
Person Responsible	Director of IT
Approval/ review body	VP-ILR
Frequency of Review*	36 months

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

Review History:		
Date of review	Reviewed by	Reason for review
Jun 2012	IT Director	General update to include staff
Oct 2015	Executive Director of Facilities and Resources	Review
Apr 2019	Executive Director of Facilities and Resources	Review
Jul 2022	Director of IT	Review

Contents

Related policies/documents:

1. Mobile Device and Communication Policy
2. Information Technology Conditions of Use Policy
3. Data Breach Policy and Procedure

NOTE – This Policy, together with the Policies and Procedures listed above, seeks 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. 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 ("the College") a multi-sited institution, which incorporates Hadlow College, is aware that malicious communication may enter the organisation via various routes and recognises that this 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.

2. Objectives

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, students, or visitors.

2.3. 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, students, or visitors in the course of their employment or involvement with the College. It may arrive by post, e-mail, phone or any other means.
Visitor:	Anyone who is not a student, or member of staff.
Harm:	Loss of or damage to a person's rights, property, or physical and/or mental well-being.

4. Types of Communication

In the modern world communication can take place using several methods including electronic and traditional means:

4.1. verbal;

4.2. written;

4.3. fax and photocopy (printed);

4.4. telephonic;

4.5. email and SMS (Text);

4.6. Social Network and blogging; and/or

4.7. mobile telephone and other devices.

5. Responsibilities

5.1. Chief Executive and Executive Principal

5.1.1. Make resources available for the operation of this policy.

5.1.2. Ensure that concerns raised by visitors relating to malicious communication are brought to the attention of the Director of IT.

5.2. Director of IT

5.2.1. Decide on the level and nature of the risk posed by any malicious communication.

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.

5.2.5. Recommend disciplinary action where appropriate.

5.3. Risk Manager/Data Protection Officer ("DPO")

5.3.1. Maintain a Central Record of Malicious Communications.

5.3.2. Collate related items of malicious communication.

5.3.3. Assist the College in assessing the potential risks posed and advise the Director of IT.

5.4. Line Managers/Lecturers

5.4.1. Adopt a supportive approach to any member of staff or student who reports that they are the subject of malicious communication.

5.4.2. Arrange for any items of malicious communication to be forwarded to the Risk Manager/DPO.

5.4.3. Advise staff or students 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 Human Resources or Student Welfare and Safeguarding Services respectively.

5.5. Staff/Students

5.5.1. Report any malicious communication, however received, to their Line Manager/Lecturer.

5.5.2. Be aware of the online social media, Internet, e-mail and telecommunications guidelines outlined in sections 5, 6, 7 and 8 of the “Information Technology Conditions of Use Policy”. Students are made aware of the College policy via the “Student Digital Learning & IT Guide”.

5.6. Visitors

5.6.1. Report any malicious communication, however received, to the Chief Executive and Executive Principal via the College’s communications channels.

6. Procedures

Anyone receiving malicious communication must bring it to the attention of their Line Manager/Tutor as soon as possible. If the communication alleges a direct and immediate threat to the health of any individual, immediately inform as appropriate Security or Estates Manager, at the campus concerned, or to the most senior manager present at any of the College’s sites. This may involve logging an incident on MyConcern if the matter directly relates to a safeguarding issue.

6.1. Communication Received by Phone

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

6.1.1. name, address, telephone number;

6.1.2. does the caller represent an organisation;

6.1.3. if the phone displays the caller ID, write down the number;

6.1.4. time, date and duration of the call;

6.1.5. the number of the phone on which the call was received;

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

6.1.7. speaker’s sex, approximate age, accent, was he/she rambling, drunk, laughing?

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

6.2. Communication Received in Written/Printed/Physical Format

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

6.3. Communication Received Electronically

DO NOT DELETE any communication received via electronic means such as emails, SMS (Texts), social networking and blogging sites or any other form of electronic communication. Inform your Line Manager/Tutor and arrange where possible, for the message to be forwarded to the Risk Manager.

6.4. 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 Risk Manager/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 any means indicated above could be regarded as gross misconduct by the College and could result in disciplinary action being taken, with possible dismissal.

Appendix 1 – Telephone Threat Record

This should be completed once the caller has hung up and you have informed Security Reception or the Director of IT 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: .....