

Whistleblowing channel policy of the University of Jyväskylä

Contents

1.	General principles	2
1.1.	Background and purpose of the policy	2
1.2.	Ownership and validity period of the policy	2
2.	Scope of the whistleblowing channel policy.....	2
3.	Reporting suspected breaches.....	2
4.	Protecting whistleblowers	3
4.1.	Prerequisites for whistleblower protection.....	3
4.2.	Ban of countermeasures	3
5.	The reception and handling process of whistleblower reports	3
5.1.	Confidential reporting in the whistleblowing channel.....	3
5.2.	Recording and retaining whistleblower reports	4
6.	Principles for arranging the whistleblowing channel.....	4
7.	Investigating whistleblower reports	4
8.	Reporting on the whistleblower system	5

1. General principles

1.1. Background and purpose of the policy

JYU takes seriously all breaches, misdemeanours and other inappropriate actions. JYU's Code of Conduct and other instructions aim at ensuring that JYU employees act in accordance with our practices and values in all situations. JYU encourages both its employees and other bodies to report observed breaches in accordance with the organisation structure or through the whistleblow channel.

The purpose of this policy is to set out principles and procedures for reporting any observed breaches and handling such reports with reference to the Whistleblower Protection Act (1171/2022). For its part, the whistleblowing channel policy supports responsible action in line with the values of the University of Jyväskylä as well as complying with the requirements set by laws and regulations.

1.2. Ownership and validity period of the policy

The University Board has approved this policy on 20 January 2023. This policy comes into force from 1 March 2023.

Decisions on specifying instructions and persons to handle the reports are made by the Rector or a person designated by the Rector.

2. Scope of the whistleblowing channel policy

This policy determines the procedures applied in dealing with whistleblower reports in accordance with the Whistleblower Protection Act. In addition to the personal coverage defined in the Whistleblower Protection Act, this policy applies to grant researchers belonging to the university community. For dealing with grievances other than those under the Whistleblower Protection Act, the University applies procedures defined in the JYU Code of Conduct or otherwise internally defined procedures at JYU.

3. Reporting suspected breaches

A report is submitted to the whistleblowing channel available on the JYU website.

JYU does not press any charges against whistleblowers due to acquiring or receiving the reported or published information, providing that such acquisition or reception is not a crime in itself.

A whistleblower report can be made without concrete evidence or full certainty of whether a breach has truly happened. However, a whistleblower who deliberately reports or publishes false information is liable to compensate any damage inflicted upon the subject of the accusation.

When the whistleblower is a JYU employee, that person should consider whether reporting the breach through the whistleblowing channel is appropriate, or if it would suffice to deal with the issue, for example, by having a discussion with one's own supervisor or someone in the management.

4. Protecting whistleblowers

4.1. Prerequisites for whistleblower protection

A report submitted to the whistleblow channel entails protection for the whistleblower in accordance with this policy. Another prerequisite for the protection is that the whistleblower has a justifiable reason to believe that the information concerning the suspected breach is correct at the time of reporting and that the reported breach is covered by the law.

4.2. Ban of countermeasures

JYU does not target any countermeasures to a person reporting suspected breaches in accordance with this whistleblowing policy. It is also forbidden to prevent or try to prevent a whistleblower from reporting a breach. Forbidden countermeasures include, for instance, weakening the person's terms of employment, terminating the employment relationship, a lay-off, or otherwise disadvantageous treatment because the person has reported breaches or suspected breaches in accordance with this whistleblowing policy or has participated in investigating the reported issue.

Forbidden countermeasures targeted at JYU's cooperation partners include, for instance, weakening the terms of cooperation, restricting or terminating the delivery of goods or services, or cutting short a contract relationship, or otherwise inflicting negative consequences because the business partner has reported observed or suspected breaches in accordance with this whistleblowing policy, or has participated in investigating the reported issue.

5. The reception and handling process of whistleblower reports

5.1. Confidential reporting in the whistleblowing channel

In the JYU whistleblowing channel, breaches are reported in writing so that the procedures in line with this policy can be secured in terms of confidentiality and whistleblower protection.

Reporting through the channel is confidential. However, JYU is not required to process any anonymous reports.

The identity of the whistleblower, the subject and other persons mentioned in the report as well as other personal data are classified information. These data can be processed by pre-assigned whistleblower report handlers or designated experts needed to investigate

the accuracy of the report. Non-authorised access to the whistleblower data is prevented by technical means.

The recipient of confidential information can disclose it only when the prerequisites defined in the Whistleblower Protection Act are fulfilled.

5.2. Recording and retaining whistleblower reports

A whistleblower is notified about the reception of the report within seven days from the date of its submission. If it is clear that a report ought not to be processed through the whistleblowing channel, the report handlers will advise the whistleblower, in line with the principles of good governance, to use other contact channels. In this connection, it must be explained to the whistleblower what consequences there are when the issue is not covered by the Whistleblower Protection Act with regard to processing, whistleblower protection, and secrecy obligations.

Personal data related to a whistleblower report are processed for as long as the report's content bears legal significance. A report will be deleted, at the latest, after five years from its arrival. Other data produced due to the report (e.g. reports, documents on the consequences) are retained or deleted according to the University's data management plan.

6. Principles for arranging the whistleblowing channel

The whistleblowing channel is designed to protect the whistleblower's identity at all stages related to filing a report. The reports are processed by report handlers specifically appointed for this task, whose names should be made public so that a potential whistleblower would know in advance who would process their report.

The report handlers must be familiar with general principles of ethical conduct, and when necessary, recuse themselves from processing a particular report.

JYU ensures that the principles of accessibility, confidentiality, data protection and information security are implemented in the whistleblowing channel. The channel is also subjected to ongoing impact assessment related to data protection and data processing. The technical framework of the whistleblowing channel must enable confidential contacts between the whistleblower and the report handlers in order to sort out the issue.

7. Investigating whistleblower reports

Those handling whistleblower reports evaluate the content of each report and request necessary additional information from the whistleblower. The report handlers' responsibilities also include making a proposal for further measures and forwarding the proposal to a competent decision-maker within JYU. The competent decision-maker is determined on the basis of the content, scope and severity of the issue concerned. Unless JYU's internal regulations for decision-making powers stipulate otherwise, the competent decision-maker is the Rector.

If a whistleblower report requires more detailed investigation, the competent decision-maker decides on the appointment of persons to investigate the accuracy of the report. If the reported breach is considered fully settled or further measures can otherwise be taken without additional investigation, no separate investigators are appointed.

Based on the work done by those handling a report or investigating its accuracy, the competent decision-maker can decide on reporting a crime, stating some other juridical claim, taking the issue to other authorities for processing, or on JYU's internal administrative sanctions.

The report handler or the competent decision-maker can decide on closing the case when, despite a request, the whistleblower does not give sufficient additional information through the whistleblowing channel. The report handler or competent decision-maker can decide to close the case also when it is about repetitive reports related to the same theme and which do not include any significant new information about the reported breach in comparison to an earlier report that has already been duly processed.

Once the investigation is completed or at the latest within three months from delivering the reception notification, the whistleblower is informed about what measures are taken based on the report.

8. Reporting on the whistleblower system

The received whistleblower reports and related steps in processing are reported to the Rector and the Director of Legal Affairs, taking into account the secrecy obligations in accordance with the Whistleblower Protection Act.

The University Board receives reports every six months on the number and nature of whistleblower reports received as well as on the resulting measures taken.