KUNGL. KONSTHÖGSKOLAN
ROYAL INSTITUTE OF ART

Guidelines for the handling of whistleblowing

Document type	Guidelines
Approved by	Vice-Chancellor
Validity	13 June 2022 – indefinite, updated 22 May 2023
Replaces document	-
Responsible administrative unit	HR

Introduction

At the Royal Institute of Art, we strive to maintain an open and transparent workplace, free from misconduct. It is therefore important to us that there is clear information on how to report concerns confidentially and securely. If there is a suspicion of ongoing or past misconduct, there must therefore be resources available to address it. By making it easy to report, we work together to safeguard the trust that staff, students and the public place in us.

1. Who can blow the whistle?

You can blow the whistle and receive protection under the Whistleblower Act if you are an employee, volunteer, intern, or a person at our disposal for work under our control and management, or if you are a member of our administrative, management or supervisory body. Contractors, subcontractors and suppliers to us who have become aware of irregularities within the university may also report them.

The fact that you have terminated your employment relationship with us, or that it has not yet commenced, does not prevent you from reporting a concern.

2. What can I report?

If you suspect a possible irregularity, we urge you to report this to us as a whistleblowing case. When reporting, it is important that you, at the time of reporting, could reasonably assume the misconduct to be true.

2.1 Misconduct in the public interest

You may report information about misconduct that has come to light in a work-related context where there is public interest in its disclosure. For other types of personal complaints where there is no public interest in their disclosure, such as disputes or complaints regarding the workplace or working environment, we urge you instead to contact your immediate manager, HR or another appropriate person in charge, or alternatively your tutor, head of department or student ombudsman. This is to ensure that these matters are handled in the best possible way.

Examples of serious misconduct that should be reported:

- Deliberately incorrect accounting, internal accounting controls or other financial crime.
- Incidents of theft, corruption, vandalism, fraud, embezzlement or data breaches.
- Serious environmental offences or major safety breaches in the workplace.

- If anyone is subjected to serious forms of discrimination or harassment.
- Other serious irregularities affecting individuals' lives or health.
- Other serious irregularities affecting the company's vital interests.

2.2 Irregularities contrary to EU law

In addition, it is possible to report information regarding irregularities arising in a work-related context that contravene EU legal acts or provisions. If you suspect that this is occurring, please read Section 2 of the Whistleblower Act and the scope of application of the Whistleblower Directive in Article 2 and Annex Part 1 for applicable laws.

3. How do I report?

3.1 Written reporting

For written reports, we use Visslan, which is our digital whistleblowing channel. It is always available via https://kkh.visslan-report.se.

On the website, select "report" to then describe the suspected misconduct. Please describe what has happened in as detail as possible, so that we can ensure appropriate measures can be taken. It is therefore also possible to attach further evidence, such as written documents, images or audio files.

3.1.1 Sensitive personal data

Please do not include sensitive personal data about individuals mentioned in your report unless it is necessary to describe your case. Sensitive personal data includes information regarding ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, a person's sex life or sexual orientation, genetic data, and biometric data used to uniquely identify a person.

3.1.2 Anonymity

You may remain anonymous throughout the process without this affecting your legal protection, but you also have the option to disclose your identity under strict confidentiality. In some cases, anonymity may make it more difficult to follow up on the case and to take the necessary measures, but in such cases, we may also ask you at a later stage to disclose your identity under strict confidentiality.

3.1.3 Follow-up & login

Once you have submitted your report, you will receive a 16-digit code, which you can use to log in to Visslan at https://kkh.visslan-report.se.

It is very important that you save the code, as otherwise you will not be able to access the case again.

If you lose the code, you can submit a new report referring to the previous one.

Within **seven days**, you will receive confirmation that the case handler has received your report. The case handler is the independent and impartial party who receives reports via the reporting channel; their contact details are provided in "6.1 Case handler contact details". If you have any questions or concerns, you and the case handler can communicate via the platform's built-in, anonymous chat function. You will receive feedback within three months regarding any measures that have been planned or implemented because of the report.

It is important that you log in at regular intervals using your 16-digit code to respond to any follow-up questions the case handler may have. In some cases, the case cannot be processed further without answers to such follow-up questions from you as the reporting person.

3.2 Verbal reporting

It is also possible to submit a verbal enquiry by uploading an audio file as an attachment when creating an enquiry on https://kkh.visslan-report.se.

In the audio file, you should describe the same circumstances and details as you would in a written report.

In addition, a face-to-face meeting with a case handler can be requested via Visslan. The easiest way to do this is either to request it within an existing report or to create a new report.

3.3 External reporting

We encourage you to always report irregularities internally first, but if difficulties arise or if it is deemed inappropriate, it is possible to make an external report instead. In such cases, we advise you to contact the competent authorities or, where applicable, EU institutions, bodies or agencies. Contact details for these can be found at the following web address: www.visslan.com/resources/visselblasarpolicy/extern-rapportering

4. What are my rights?

4.1 Right to confidentiality

Throughout the handling of the case, we will ensure that your identity as the reporting person is treated confidentially and that unauthorized staff are prevented from accessing the case. We will not disclose your identity without your consent unless required to do so by applicable legislation, and we will ensure that you are not subjected to reprisals.

4.2 Protection against reprisals

In the event of whistleblowing, there is protection against negative consequences arising from reporting a breach, in the form of a prohibition on reprisals. Protection against reprisals also applies, where relevant, to people in the workplace who assist the reporting person, your colleagues and relatives in the workplace, and legal entities that you own, work for or are otherwise associated with.

This means that threats of reprisals and attempts at reprisals are not permitted. Examples of this include being dismissed, having your duties changed, being subjected to disciplinary measures, being threatened, discriminated against, blacklisted within your industry, or similar actions because you blew the whistle.

Even if you were to be identified and subjected to reprisals, you would still be covered by protection, provided you had reasonable grounds to believe that the irregularity reported was true and fell within the scope of the Whistleblower Act. Note, however, that protection is not granted if it is a criminal offence to obtain or have access to the information reported.

Protection against reprisals also applies in legal proceedings, including those relating to defamation, copyright infringement, breaches of professional secrecy, breaches of data protection rules, disclosure of trade secrets, or claims for damages based on private law, public law or collective labor law, and you shall not be held liable in any way as a result of reports or disclosures, provided that you had reasonable grounds to believe that it was necessary to report or disclose such information in order to reveal a wrongdoing.

4.3 Disclosure of information

This protection also applies to the disclosure of information. This is subject to the condition that you have reported the matter internally within the company and externally to an authority, or directly externally, and no appropriate action has been taken within three months (or six months in justified cases). Protection is also granted if you have reasonable grounds to believe that there may be a clear danger to public interest if the information is not disclosed, for example in an emergency. The same applies where, in the case of external reporting, there is a risk of reprisals, or it is unlikely that the

irregularity will be effectively remedied, for example where there is a risk that evidence may be concealed or destroyed.

Please note, however, that this protection does not apply if you, as the reporting person, disclose information directly to the media in accordance with an otherwise applicable system of protection for freedom of expression and information. You therefore still have whistleblower protection and freedom of access to information where applicable.

4.4 Right to review documentation during meetings with case handlers

If you have requested a meeting with a case handler, they will, with your consent, ensure that a complete and accurate record of the meeting is kept in a durable and accessible form. This may be done, for example, by recording the conversation or by taking minutes. Afterwards, you will have the opportunity to check, correct and approve the minutes by signing them.

If the conversation was not recorded, the case handler has the right to document the conversation by taking minutes. Afterwards, you will have the opportunity to review, correct and approve the transcript by signing it.

We recommend that this documentation is kept on the Visslan platform by the whistleblower to create a case where the information can be collected securely.

5. The GDPR and the processing of personal data

We always do our utmost to protect you and your personal data. We therefore ensure that our processing of such data is always in accordance with the General Data Protection Regulation ("GDPR").

In addition, all personal data not relevant to the case will be deleted, and the case will only be retained for as long as is necessary and proportionate to do so. At the very latest, a case may be processed for two years after its closure.

6. Further contact

If you have any further questions regarding how we handle whistleblowing cases, you are always welcome to contact the case handler.

If you have any technical queries regarding the Visslan platform, please create a ticket at https://kkh.visslan-report.se. If this is not possible, please contact Okapia AB, the developers of Visslan. Contact details for both are provided below.

6.1 Contact details for the case manager

Position: Head of HR

Telephone number: 08-614 40 00

If the Head of HR is unavailable, the Head of the Education and Research Unit will act as the case handler.

Telephone number: 08-614 40 00

6.2 Contact details for Okapia AB

Email: clientsupport@visslan.se

Switchboard number: +46 10-750 08 10