Rules for handling official documents

Guidance for the application of regulations on official documents and public access to information and secrecy at Karlstad University[1]

[1] This document has been drafted on the basis of current legislation. If laws or regulations are amended, or if the provisions of this document deviate from current law, laws and regulations shall always prevail.

Decision	RB 80/26	Dnr.	2026/556	Replaces	C2019/966
Validity from	2026-08-31	even	Until further notice	Administrators	Emma Engh

Table of Contents

Rules for handling official documents 1
1. The principle of public access to official documents 4
2. The principle of public access to official documents and the General Data Protection Regulation 4
3. What is an official document? 4
4. Public access to information and secrecy 5
4.1 Information classified as secret 6
4.2 Handling of secret documents 7
4.3 Prohibition on disclosing secret information 8
4.4 Privacy and information security 8
4.5 How is secrecy assessed? 9
4.6 Specific information about exams 9
5. Providing an official document 10
5.1 Request for an official document 10
5.2 Who makes the decision on the disclosure of an official document? 10
5.3 Anonymity 11
5.4 How is disclosure made? 11
5.4.1 Released on paper or in electronic form 11
5.4.2 Security when disclosing official documents 11
5.4.3 Electronic disclosure of personal data 12
5.4.4 Disclosure of information from official documents 12
5.4.5 Disclosure of data from Ladok 12
5.5 Denying access 12
5.6 Decisions on disclosure with reservations, etc. 13
5.7 Should we charge for copies? 13
6. Registration 13
6.1 General information about diary 13
6.2 Registration stations and series 14
6.3 What should be registered? 14
6.4 When should official documents be registered? 14
6.5 Should documents sent internally be registered? 15
6.6 Documents of minor importance 15
6.7 Documents that are kept in order in a way other than by registration 15
7. Mail handling 16

7.1 Personally addressed mail 16
8. E-mail as an official document 16
8.1 Official documents 16
8.2 Private email 17
8.3 Registration of e-mail 17
8.4 Accessibility 18
8.5 Deletion of e-mails 18
8.5.1 Recycled bin (Deleted items) 19
8.5.2 Email logs 19
8.5.3 Backups 19
8.6 Secrecy in e-mails 20

1. The principle of public access to official documents

The principle of public access to official documents means that the public and the mass media have the right to insight into the activities of public authorities. This transparency can be expressed in different ways and in different forms, for example through freedom of expression, freedom of the press, freedom of information and publicity in court proceedings. Another example of such a right of access is the public access to official document.

Public access to documents means that as a general rule everyone, both Swedish and foreign citizens, has the right to access the documents stored by Swedish authorities. This right is limited in only two ways. First, not all documents stored by an authority are official documents, and second, some official documents are covered by secrecy.

2. The principle of public access to official documents and the General Data Protection Regulation

The General Data Protection Regulation (GDPR) (EU) 2016/679 has been in force as law in all EU member states since 25 May 2018. The regulation entails a lot of requirements for those who process personal data as well as rights for the individual in terms of personal privacy.

Karlstad University is the data controller for the processing of personal data that takes place in its operations. All processing of personal data must comply with the basic principles set out in the General Data Protection Regulation. In simple terms, the principles mean that personal data may only be collected for certain legitimate purposes, that no more data than necessary may be processed and that the data may not be stored for longer than necessary.

However, the General Data Protection Regulation does not prevent the processing of personal data that is necessary for public authorities to be able to fulfil obligations in accordance with the principle of public access to official documents.

3. What is an official document?

Chapter 2, Section 1 of the Freedom of the Press Act (TF) states that Swedish citizens have the right to access official documents[2]. In order for an authority to be able to decide what is to be disclosed, it is therefore necessary to know what is meant by the terms document and official document.

A document refers to a written or visual presentation or a recording that can be read, listened to or otherwise understood only with technical aids. The term document thus denotes not only an ordinary paper document with writing or images, but also, for example, tape recordings and electronically stored material. The right to access documents is independent of the medium on which they have been created. The decisive factor is the content – not the way in which the information has been fixed. It can therefore be briefly expressed that a document is an object that contains information of some kind.

[2] For foreign citizens, there is a corresponding right according to Chapter 14. 5 of the Freedom of the Press Act, as long as nothing else follows from the Freedom of the Press Act or other law.

As a general rule, all documents are official if they:
1. are held by the Authority, and
2. are considered to have been received by the authority or drawn up by the authority.

Held means that a document can be read, listened to or otherwise perceived by the authority with technical aids. However, the document does not have to be physically at the authority to be considered held there. If, for example, a document is temporarily stored at an employee's home or stored with someone else from whom the authority can easily reclaim the document, it is still considered to be held at the authority.

A document is considered to have been received by the authority when it has arrived at the authority or has been received by an authorised official. This means that documents sent to the university by post become official as soon as they arrive. If a document is not sent directly to the authority's central address, but is instead delivered in person or sent to an employee's home address, it is received when it has been received by an employee of the authority. It is therefore of no importance where the employee is when he or she receives the document. However, messages addressed in person to officials at a public authority are not official documents if the content is not work-related but relates to purely personal matters.

As a general rule, a document produced within an authority is considered to have been drawn up when it has been dispatched, i.e. sent from the authority or made available for collection. A document that has not been dispatched is drawn up when the matter to which the document belongs has been finalised by the authority. If the document does not belong to a specific matter, it is considered to have been drawn up when it has been adjusted or completed in some other way.

For certain types of documents, special rules apply as to when they are considered to have been drawn up. This applies, for example, to diaries and other lists where continuous entries are made that are considered to have been drawn up when the document is ready for use, judgments and decisions that are considered to have been drawn up when they are pronounced or dispatched, as well as official minutes and comparable documents that are considered to have been drawn up when they have been adjusted or completed in some other way.

Memos, drafts or other work documents are not considered to be official documents, provided that they are not dispatched or taken care of for archiving.

In TF there are many rules about when a document is considered to have been drawn up by an authority, which can lead to difficult assessment questions. In case of doubt, the registrar or university lawyer should therefore be consulted.

4. Public access to information and secrecy

Official documents can either be public or secret. The starting point is that an official document is public. In some cases, however, there may be reason to limit the right to access the information contained in an official document. According to the Freedom of the Press Act, such a restriction must be specified in a special law (Chapter 2, Section 2 of the Freedom of the Press Act).

It is the rules in the Public Access to Information and Secrecy Act (2009:400) (OSL) that determine whether an official document is public or not. In order for secrecy to apply to information in an official document, there must always be a specific legal basis in the OSL and the issue of confidentiality must be examined in each individual case.

The fact that information is confidential means that it is prohibited to disclose the information, whether orally, through disclosure of an official document or in any other way (Chapter 3, Section 1
§ OSL). It is not required that the information is documented in an official document in order for it to be confidential. Oral information that has not yet been recorded and information in documents that are not official may also be of the kind that they are confidential.

The prohibition on disclosing confidential information applies both to the public and to other authorities. As a general rule, the prohibition also applies within the authority. Only the employee(s) who need the information to carry out their work have the right to access confidential information.

4.1 Information classified as secret

In order to classify information in an official document as secret, there must be a legal rule in the Public Access to Information and Secrecy Act on which one can rely. If there is no section of the Act to invoke, the document is public (Chapter 2, Section 2 of the Act on Public Access to Information and Secrecy, Chapter 8, Section 1 of the OSL).

When an official document is requested, a secrecy assessment must be made in each individual case. However, the authority can already indicate that information in a document is covered by a provision on secrecy by means of a special note on the document (confidentiality/secrecy marking). Such a note acts as a warning bell. In the event of a request for disclosure of the document, it is then assessed whether the information may be disclosed or whether it is covered by secrecy.

Examples of secrecy
Secrecy applies to personal data according to Chapter 21, Section 7 of the OSL, if it can be assumed that disclosure would result in the data being processed in violation of the General Data Protection Regulation or without the necessary approval in accordance with the Act (2003:460) on the Ethical Review of Research Relating to Human Beings. Before disclosure takes place, it must therefore be assessed how the person receiving the personal data will process it. If it can be assumed that the data will be processed in violation of the General Data Protection Regulation, it may not be disclosed.

Serecy applies to information about **individuals' personal circumstances** in sociological, psychological, educational or other behavioural or social science studies (Section 7 of the Public Access to Information and Secrecy Ordinance (2009:641) and Chapter 24, Section 8 of the OSL).

Secrecy may apply to information provided by companies in connection with **commissioned research or thesis work**. Confidentiality applies if it must be assumed that the assignment has been provided provided that the information is not disclosed (Chapter 31, Section 12 OSL). The extent of confidentiality is usually specified in the assignment

agreements entered into between the University and the client.

Information obtained by companies in **collaborative projects** is also covered by secrecy according to Chapter 24, Section 5 of the OSL: "Secrecy applies to universities and colleges for information about an individual's business or operating conditions, inventions or research results that have been provided or come to light in such research that is conducted in collaboration with an individual by agreement, if it must be assumed that the individual has participated in the collaboration, provided that the information is not disclosed".

Information in **personnel social and personnel administrative activities** , about individuals' personal circumstances, medical information, private residential addresses, etc., is covered by secrecy (Chapter 39, Sections 1-3 of the OSL).

Secrecy applies to information concerning an **individual's health or sexual life**, such as information about diseases, substance abuse, sexual orientation, gender reassignment, sexual offences or other similar information, if it must be assumed that the individual or someone close to him or her will suffer significantly but if the information is disclosed (Chapter 21, Section 1 of the OSL).

Secrecy applies to information about an individual student's identity, address and other similar information if it can be assumed for special reasons that the individual or someone close to the individual is suffering but if the information is disclosed (Chapter 23, Section 5, second paragraph, OSL). For various reasons, a student may need **a protected identity** and may then be assigned a so-called alias in the study documentation system Ladok to avoid identification. Questions about the confidentiality of students' personal data are referred to the official responsible for Ladok. [3]

Secrecy also applies in "**library activities** for information in registers about an individual's loans, reservations or other forms of order and for information about an individual's use of information technology" (Chapter 40, Section 3 of the OSL).

4.2 Handling of secret documents

Appendix 1 provides examples of provisions in the Public Access to Information and Secrecy Act that may be relevant to the University's operations.

It is normally the expert (e.g. the administrator or researcher) who can assess whether a document received or drawn up contains secret information and should therefore be marked with "Confidentiality". Such a note must also state the applicable secrecy provision, the date when the note was made, and that the note was made by Karlstad University (Chapter 5, Section 5 OSL).

As a general rule, the following procedure applies to documents containing information from companies that have been submitted in connection with assignments or collabora-

[3] A memo with information about the procedures for protecting students' identity can be found at the person responsible for the student register and on the intranet, "Handling of data about students with protected personal data".

tive projects. The company itself must, in accordance with the provisions of the agreement with the University, make a note on a document if it contains confidential information. If the company has not made a note of confidentiality on the document, an expert must assess the content of the document and, if necessary, ensure that it is marked with "Confidentiality".

For documents covered by secrecy, there is an absolute registration requirement, but the registration must be done in such a way that no secret information is revealed (Chapter 5, Sections 1 and 2 of the OSL). When registering, the applicable secrecy provision and the date on which the entry was made are marked in the system. When registering, information about the sender, recipient and content may be omitted if necessary with regard to the secrecy requirement.

The fact that secret documents must be registered has to do with ensuring that the authority has good control of its secret documents and that it is easy to determine which secret documents an authority has.

4.3 Prohibition on disclosing secret information

The prohibition on disclosing secret information applies to the University as a public authority and to employees or others who participate or have participated in the activities and then become aware of the information (Chapter 2, Section 1 of the OSL). An employee who leaves must therefore observe secrecy even after the employment has ended.

As a general rule, the prohibition on disclosing secret information also applies within the University. Only the person who handles a case or otherwise participates in the processing of a case, or for some other reason must have access to the information in order to carry out their work, has the right to access the information that is secret.

In the event of a breach of confidentiality provisions, the University may be liable for damages in accordance with provisions in agreements or statutory rules. The person who has disclosed confidential information may also be liable for damages in some cases, depending on the circumstances.

A fine may be imposed for breach of the duty of secrecy through negligence. If there is intent, the penalty may be a fine or imprisonment for a maximum of one year (Chapter 20, Section 3 of the Penal Code).

4.4 Privacy and information security

Secret information must be handled in services that Kau has assessed to meet the requirements for adequate security. The assessment is based on the University's guidelines for information security and includes, among other things, protection against unauthorised access. Only those people who need the information to perform their duties should have access. This means that access must be limited and controlled so that the information is not spread to unauthorised persons.

4.5 How is secrecy assessed?

When deciding whether the information in an official document is covered by secrecy, it must be done with direct reference to a section of OSL. This means that there must be an explicit provision in OSL that protects the information in question. However, the rules of the law are generally not unconditional. Secrecy is often limited in time and must be examined on a case-by-case basis in a special damage assessment. This can lead to difficult assessment questions. In case of uncertainty, the registrar or university lawyer should therefore be contacted.

When assessing whether a piece of information is to be regarded as secret, it must first be examined whether the information is covered by any secrecy provision in the OSL. An assessment must then be made as to whether the specific provision is applicable based on what information it covers, what activities it applies to and what damage could occur if the information in question were nevertheless disclosed (damage assessment). Such a damage assessment is made on the basis of the conditions set out in the secrecy provision, so-called damage requisites. Depending on how the damage condition is formulated, the main rule is publicity for certain secrecy provisions and secrecy for other provisions.

The duration of secrecy is stated in each provision and is set at a certain number of years, e.g. ten, fifty or seventy years. This is because the risk of harm generally decreases over time. Within the specified time frame, the question of whether information can be disclosed must be assessed on the basis of the risk of harm that exists at the time of the request for disclosure.

4.6 Specific information about exams

When the examination takes place in written form, the questionnaire becomes an official document the moment it is handed over, i.e. dispatched, to the students who participate in the examination. There may be reasons to refuse to disclose the questionnaire before the examination has been conducted. The basis for this is a specific secrecy provision that applies to examinations (Chapter 17, Section 3c of the OSL):

"Secrecy applies to information that is part of or forms the basis for a knowledge test or psychological test under the supervision of an authority, if it can be assumed that the purpose of the test will be counteracted if the information is disclosed."

Secrecy applies during the time the test is in progress. After the test has been completed, the questionnaire is usually made public because the risk of injury has disappeared.[4]

Exam answers that students submit to a higher education institution are a document received and thus official. There is no confidentiality for submitted exams and anyone has the right to read or receive a copy of the exam writing.[5]

---

[4] The exception is, for example, standardised tests that are designed to be reused in part or in their entirety. Information in such tests may be confidential for a longer period of time.

[5] See, however, the Parliamentary Ombudsman's decision of 18 July 1991, ref. no. 3980-1990. The Parliamentary Ombudsman is of the opinion that an examination written by the examiner, with comments imposed by the examiner, should be regarded as a document drawn up by the higher education institution and therefore does not need to be disclosed before grades have been determined.

5. Providing an official document

5.1 Request for an official document

If someone wants to take part in a document, there are primarily two questions to consider:

1) Is the document official or not?
2) Is the document public or not?

If the document is not official, it does not need to be disclosed. You can disclose it if you want to (and provided that it does not contain secret information), but no one can demand to see it on the basis of the principle of public access to official documents.

Official and public
If the document is official and public, it must be disclosed "immediately or as soon as possible" to the person requesting the document so that it can be read, listened to or otherwise perceived. The document must be made available free of charge on the authority's premises (Chapter 2, Section 12
§ TF).

A person who requests it also has the right to receive a printout or a copy of an official document for a fee. Such a request must be processed promptly (Chapter 2, Section 16).

Official but confidential
If the document is official but secret, the document may not be disclosed.

If the document is partially secret, the public parts must be disclosed by releasing a copy of the document with the secret parts masked.

Please note that secrecy for the protection of individuals does not generally apply in relation to the individual himself. This means that secret information may be disclosed to the person to whom the personal data relates, and that the individual can also consent to such information being disclosed to others. However, this applies provided that nothing else follows from a provision in the Public Access to Information and Secrecy Act (Chapter 12, Sections 1-2 of the OSL).

5.2 Who makes the decision on the disclosure of an official document?

A request for disclosure of an official document must be processed promptly, which preferably means the same day. Normally, it can take one to two working days, and in the case of more complicated assessments, it can take longer.

In many cases, disclosure of public documents takes place without any assessment problems. Some documents can be disclosed almost routinely, e.g. old exams, course syllabi, course evaluations, etc.

A decision that an official document may be disclosed is therefore primarily made by the employee who is in charge of/responsible for the document or by the respective registrar or the main registrar (Chapter 6, Section 3 of the OSL). If you feel unsure, you

should consult your immediate supervisor, the main registrar or the university lawyer. This must be done immediately.

Appendix 2 contains a schematic picture of the assessment of whether a document should be disclosed or not.

5.3 Anonymity

A person requesting official documents normally has the right to remain anonymous. The authority may not ask about the person's identity or for what reason the person wants to access the document. The only exception is to the extent necessary for the authority to be able to carry out a confidentiality assessment (Chapter 2, Section 14 of the Act on Secrecy).

5.4 How is disclosure made?

5.4.1 Released on paper or in electronic form

According to the Freedom of the Press Act, a person who requests an official document has the right to access the document on the authority's premises, and to receive a printout or copy of the document for a fixed fee. There is no obligation for an authority to disclose public documents in electronic form (e.g. e-mail, upload to a website, text message, USB stick).

However, the fact that public documents do not need to be disclosed electronically under the Freedom of the Press Act does not mean that the University is always prevented from disclosing documents electronically. In line with the authority's service obligation under the Administrative Procedure Act, the University may disclose public documents electronically to anyone who requests it, provided that this is not inappropriate. However, before an electronic disclosure takes place, it must always be assessed whether such disclosure is appropriate and compatible with, for example, the General Data Protection Regulation.

5.4.2 Security when disclosing official documents

When official documents are released, whether on paper or electronically, it must be done in a way that ensures that the document reaches the right recipient and does not risk ending up in the wrong hands.

In electronic disclosure, the services and communication methods that Kau deems to be sufficiently secure must be used. Employees must therefore always follow the University's internal guidelines and use the appropriate solutions.

When dispensing on paper, the disclosure must be handled in such a way that the risk of error or loss is minimized. This means, among other things, checking the correct address and using appropriate packaging.

5.4.3 Electronic disclosure of personal data

Please note that there is no obligation under Swedish law to disclose public documents in electronic form. If Karlstad University is to disclose documents containing personal data electronically, the University must therefore ensure that all requirements of the General Data Protection Regulation are met. This means that the possibilities of disclosing personal data in electronic form are severely limited.

An assessment must be made in each individual case, but the main rule at Karlstad University is that sensitive personal data, information about criminal convictions, personal identity numbers and other privacy-sensitive data, as well as bulk extraction of personal data, are not disclosed electronically. Other types of personal data may in some cases – provided that the University deems it appropriate and in accordance with the rules of the General Data Protection Regulation – be disclosed, e.g. by e-mail.

It is always Karlstad University, in its capacity as data controller, that unilaterally makes the assessment of whether a document should be disclosed electronically or not. The decision cannot be appealed.

5.4.4 Disclosure of information from official documents

In addition to the right to access official documents, it is also possible to request information from official documents. This is not regulated in the Freedom of the Press Act, but follows from the Public Access to Information and Secrecy Act. According to Chapter 6. Section 4 of the OSL, an authority shall, upon request, disclose information from public documents stored by the authority, "unless the information is confidential or it would impede the proper course of the work". The manner in which a request is to be answered by the authority may be determined in the light of the circumstances.

5.4.5 Disclosure of data from Ladok

As regards information from the Ladok study register, these may only be disclosed electronically in cases specifically listed in the Ordinance (1993:1153) on the reporting of studies etc. at universities and colleges.

5.5 Denying access

If the person processing a request for disclosure of an official document assesses that the document cannot be disclosed, or can only be disclosed with reservations or other restrictions, he or she must inform of the right to an appealable written decision. If the applicant requests a written decision, the main registrar or university lawyer must be contacted immediately.

If someone asks for a document that is confidential, this must be notified, for example in the following ways:

"In our assessment, the document you have requested access to unfortunately cannot be disclosed due to secrecy according to **chapter**, **paragraph**§ of the Public Access to Information and Secrecy Act. If you are not satisfied with the information, you can

request that the authority examine the matter and thus receive an appealable written decision."

The written decision of the authority is made by the Vice-Chancellor with justification and reference to the rule that is applied. The decision can be appealed and an appeal reference must be attached to the decision. The appeal body for appeals is the Administrative Court of Appeal in Gothenburg.

5.6 Decisions on disclosure with reservations, etc.

If it is relevant to disclose secret documents with reservations, a decision must be made by the Vice-Chancellor. This also applies if it is relevant to disclose confidential documents after the individual to whom the information relates has given his/her consent to the disclosure or the individual requests confidential information about him/herself.

5.7 Should we charge for copies?

In addition to the right to access an official document on site, you also have the right to receive a printout or copy of the document. If an order is ten pages or more, a fee must be charged. The fee for an order of ten pages is SEK 50. For each page in addition, the fee is SEK 2. Compensation for postage costs must also be charged if the item weighs more than 20 grams (Sections 15-22 of the Fees Ordinance).

There is no regulation in the Fees Ordinance that specifically aims at the disclosure of public documents in electronic form, but according to court practice, it may be possible to charge such disclosure as well.[6]

6. Registration

6.1 General information about diary

A registry (*diarium*) is a register of an authority's official documents. Registering official documents is a practical way to keep documents organised in order to be able to find them quickly and to get a relatively easy overview of which official documents have been received or drawn up.

The special thing about a registry, in relation to other types of registers, is that in a registry, all documents in a case are kept together and assigned a common registration number. All documents in a case must be registered under one and the same registration number, regardless of when they are received.

[6] See the Administrative Court of Appeal in Stockholm, case no. 4805-14. It follows from Section 4 of the Fees Ordinance that an authority may, for a fee, provide, among other things, automatic data processing information in a form other than printing. For fees levied under this provision, the authority may, within the framework of full cost coverage, decide on the grounds for setting the fee (Section 5 of the Fees Ordinance).

6.2 Registration stations and series

Karlstad University registers its public documents in an electronic case management system. Registration takes place at so-called registry stations, and they are located at the Faculty of Health, Science and Technology, the Faculty of Arts and Social Sciences, the Office of Teacher Education and at central support functions (including the University Library). Everyone has their own series in the registry itself.

Although the registry stations are in practice independent of each other, they are actually parts of a single registry. Authorized persons in the system can thus go in and search the entire registry for cases and documents and obtain the information needed. The division is purely for practical reasons and does not mean that the registry units would be independent in relation to each other. They are all part of Karlstad University as a public authority.

An official document should not be registered in more than one series. The reason for this is that otherwise it can easily arise problems with knowing where the document itself should be stored.

A large part of the University's public documents are kept organised in other ways than in the registry. Other documents are registered in registers other than the registry, for example in the student register, the financial system and the staff recruitment system.

6.3 What should be registered?

The main rule is that all public documents must be registered. The exception is documents that are produced in large quantities and that can be kept in order in another way. Examples of what must be registered can be found in Appendix 3. In case of uncertainty, the registrar must be contacted.

The Freedom of the Press Act defines a document as "a written or visual presentation and a recording that can be read, listened to or otherwise understood only by technical means" (Chapter 2, Section 3 of the Freedom of the Press Act). In other words, in addition to paper documents, information stored digitally, photos and sound recordings can also be public documents.

Documents sent from the University are considered to be prepared and thus public documents when they are dispatched. A document must be registered with a registration number before it leaves the University and a copy (single-sided according to RA-FS 2010:2). RA-FS 2010:2) must be archived.

6.4 When should official documents be registered?

Official documents must be registered as soon as they have been received by or prepared by an authority (Chapter 5, Section 1 of the OSL).

This means that an incoming official document should be registered on the same day as it is received by the authority or received by the relevant official, preferably in direct connection with the opening of the mail (letter, e-mail, text message) or submission.

Mail handling at the University must therefore be managed in an efficient manner. All mail should be opened and date-stamped on the same day as they arrive. This also applies to directly addressed mail and mail that is delivered to employees at their home address or at a place other than the University if the mail concerns official matters.

6.5 Should documents sent internally be registered?

In some cases, some documents may be considered to be prepared when they are dispatched internally, such as minutes, decisions or information about measures to be implemented. Such prepared documents must therefore be registered in connection with their sent. If the document is sent to Central Support Functions, it must be registered there.

Documents such as draft decisions or internal referrals that are sent between faculties/divisions are not official documents and do not need to be registered (Chapter 2, Section 8 of the TF).

6.6 Documents of minor importance

If it is obvious that an official document is of minor importance to the authority's activities, it does not need to be registered. These documents can be disposed of when they are not needed for the activities.

Some examples:

- Advertising brochures
- Invitations to courses and conferences
- Circular and legislative printing
- Routine requests (e.g., course offerings)
- Minutes received for information (original is kept where it has been drawn up)
- Invitations

6.7 Documents that are kept in order in a way other than by registration

There are official documents that are of such a nature that they are produced in relatively large quantities and/or are of a routine nature. Official documents of this kind are not usually registered, but in such cases the documents are kept in order in another way.

When it comes to the question of which documents should be registered and which should be kept in order in some other way, it is important that the procedures are as uniform and consistent as possible.

It is also important to keep in mind that in cases where official documents are not registered, this does not mean that they can be handled in any manner whatsoever. Even in the case of these documents, it should be possible to determine without difficulty whether they have been received or drawn up, and it should be possible to quickly find and retrieve individual official documents that have not been registered if someone asks for them. The easiest way to keep documents organised in another way is to collect them in one place. You can sort by chronological, alphabetical or numerical order.

7. Mail handling

At Karlstad University, mail is opened at the faculties, the Teacher Education Board's office and at the departments of central support functions. A designated person, with knowledge of the applicable rules, opens the mail, date stamps and registers relevant documents and sorts the mail to the addressee. The person who opens the mail is always obliged to decide whether the document should be registered. This applies to both paper mail and e-mail.

7.1 Personally addressed mail

Employees at the University shall, as far as possible, avoid private mail to and from the University. Mail opening must be handled by appointed administrators who have knowledge of the applicable rules. Mail addressed with a personal name before the name of the authority may not be opened without the addressee's special consent. In order to comply with the law's requirements for rapid registration and at the same time protect personal integrity, it is advisable for the staff to authorise the appointed administrator to open all mail received by the University.

If an employee has not provided a power of attorney, the administrator must not open personally addressed mail. In order for the law's requirements for rapid registration of official documents to still be met, it is important that the individual employee provides himself with the necessary knowledge to assess the need for registration of documents and to ensure that the documents are received by the registrar as soon as possible.

Managers are responsible for following up that staff are informed of the obligation to register official documents without delay.

8. E-mail as an official document

E-mails received in the course of service to employees of the University from senders outside the University are seen as received by the authority and thus official documents to the same extent as conventional mail. According to the principle of public access to official documents, this means that anyone has the right to access such messages, provided that the content is not secret, and that the authority is obliged to consider a request to receive such messages upon request in the same way as for other incoming mail to the authority.

8.1 Official documents

E-mail received at Karlstad University from another authority or individual becomes an official document as soon as it has arrived on one of Kau's e-mail servers, if the message in any part relates to a matter or a question about the authority's activities.

E-mails sent from Karlstad University to an external addressee are considered to have been dispatched (sent) and are thus drawn up. It is of no importance whether the content of the document is intended to be completed or not.

As a general rule, e-mails that are only sent internally within Kau do not become a public document due to the e-mail being sent. The same applies to SMS and MMS between work mobiles.

SMS and MMS in and out of the authority's work mobiles can also be considered as public documents in the same way as e-mail.

The information about messages contained in logs/lists is always public document.

E-mails stored in Kau's e-mail system are considered to be held by the authority.

Exceptions
Some documents never become official unless they are taken care of for archiving. For example, draft decisions in a case, memos that have not added a concrete information to a case or internal information mailings.

8.2 Private email

As a general rule, employees at Karlstad University should not use the university's e-mail address for private matters, as it can be difficult for the correspondent to distinguish between the official at the authority and the private individual. If an employee uses the university's e-mail address for private messages, these must be placed in a separate folder marked "Private". All e-mail at the university is covered by the principle of public access to official documents. It is therefore important to be able to distinguish private e-mail from the authority's. Even if private e-mail is not a public document, the log containing the sender, title and time, among other things, is an official and public document, even for the private e-mail that may be included therein.

8.3 Registration of e-mail

E-mail must be registered to the same extent as conventional mail, incoming and outgoing. In this way, it will be possible both to provide an official document immediately on request in accordance with the requirements of the law and to internally overview which documents are available at the authority.

E-mails received by or sent from an e-mail system that are to be registered must be forwarded to the registrar immediately. Please note that any appendices must be included. The registrar registers e-mails in accordance with current rules. If the e-mail relates to a new case, the registrar must send a confirmation to the administrator with information about the registration number , etc.

Examples of public documents that do not need to be registered:

- Documents which have been submitted for information only and which have not given rise to any action.
- Enquiries and messages that are of temporary or minor importance. Please note that the document's minor significance to the university’s operations must be obvious. In case of doubt, it should be registered.
- Routine invitations to conferences, courses and seminars aimed at multiple recipients.
- Routine requests (e.g., "When is the exam?").
- Documents that according to the current information management plan must be kept in another register or kept in order in some other way.

The log of incoming and outgoing e-mails in itself is considered an official document and the list as such does not have any secrecy protection. This means, for example, that a journalist who wants to access an employee's log has the right to do so. The separate e-mails, on the other hand, are assessed separately in accordance with what has previously been stated regarding the status of an official document or not and about any secrecy protection for the content.

8.4 Accessibility

E-mails relating to Kau's activities must always be handled in accordance with applicable laws and regulations, even in the event of absence. It must be possible to register and examine any request of official documents immediately. Questions from the public must be answered as soon as possible.

It is important that the e-mail is monitored regularly, either by the employee himself or by a colleague. In the event of vacation or short absence, the "auto-reply" function must also be used to notify the period during which the person in question is absent and to refer to an alternative e-mail address (colleague's e-mail address or suitable functional address). In the case of longer absences, such as leave of absence, a decision is made on how the e-mail is to be handled in consultation with the responsible supervisor.

8.5 Deletion of e-mails

Official documents received by e-mail may be deleted in accordance with the rules in the University's information management plan. Official documents may only be deleted in accordance with regulations and decisions by the National Archives. If the e-mail constitutes an official document that is to be preserved and registered in the registry or other computer system, it must be transferred to another data carrier and deleted from the university's own e-mail system after it has been sent to the registrar or transferred to another computer system.

An e-mail directory is not a place for storing and archiving official documents. It can be compared to mail sorting and our physical mailboxes. If, for example, a sick note is received by e-mail, it must be transferred to the relevant personnel system and then deleted from the e-mail system.

All e-mail handling also involves the processing of personal data. According to the General Data Protection Regulation, personal data may not be stored in a form that enables the identification of a natural person for a longer period than is necessary for the purposes for which the personal data is processed.

Note that e-mails are official documents as long as they remain. No e-mails may be deleted automatically, but must be reviewed manually before deletion, with the exception of the central spam management.

In the e-mail system, there may be documents that are not public and when they are deleted, the term “clearing” (*sw gallring*) is used. The following are examples of documents that are not public and can therefore be cleared:

- Drafts, "drafts", concepts and other documentation for not yet completed/prepared letters and decisions that are exchanged within the authority as working material during the preparation of a case. However, there may be situations when an internal e-mail may relate to a specific matter at the authority and should be added to the case. In such a case, the document should be registered and placed in the file and then become a public document.
- Memos, which means that they belong to a case without adding factual information to the case and that they have not been dispatched or archived
- Internal referrals, i.e. drafts and proposals that are sent from one authority to another authority for consultation purposes. These should therefore not be registered.
- Intra-agency announcements and information releases
- Purely personal messages and of an obviously private nature
- Documents received by a person in the capacity of another position, such as internal party mail to a politician or mail to a trade union shop steward. Trade union mail, i.e. information provided by a trade union organisation to a site representative at a public authority, is not public documents.

The inbox and outbox must be regularly cleaned of files that are not official documents and the trash can must be emptied regularly.

8.5.1 Recycled bin (Deleted items)

"Junk mail", such as mass advertising, "spam" and irrelevant messages that have nothing to do with the University's operations, can be deleted immediately.

Please note, however, that everything that is in the Recycled Bin (Deleted Items/Trash) is to be considered as undeleted, i.e. still a public document.

8.5.2 Email logs

E-mail logs are compilations of incoming and outgoing e-mail. The logs contain information about the sender (server and e-mail), recipient, message ID, date and subject line.

They are to be regarded as a type of action of minor or temporary importance and are automatically discarded in the event of incompetence.

8.5.3 Backups

The purpose of backup is to be able to restore the information if the original information on the IT system is damaged or has been accidentally deleted. How long it is possible to restore a backup, or how often the backups are taken, is determined by the requirements set by the IT system.

In some IT systems, the user can restore information from the backups themselves.
In other IT systems, only IT staff can restore information from the backups.

A backup (also referred to as a backup) in itself is not a public document.

8.6 Secrecy in e-mails

Secret documents must always be registered. E-mails containing information that may be protected by secrecy must be printed and registered. After that, the message must be deleted from the e-mail system and the Recycle Bin.

Any information sent electronically can be leaked to anyone other than the intended recipient. Therefore, confidential information should not be sent by e-mail.

Appendix 1

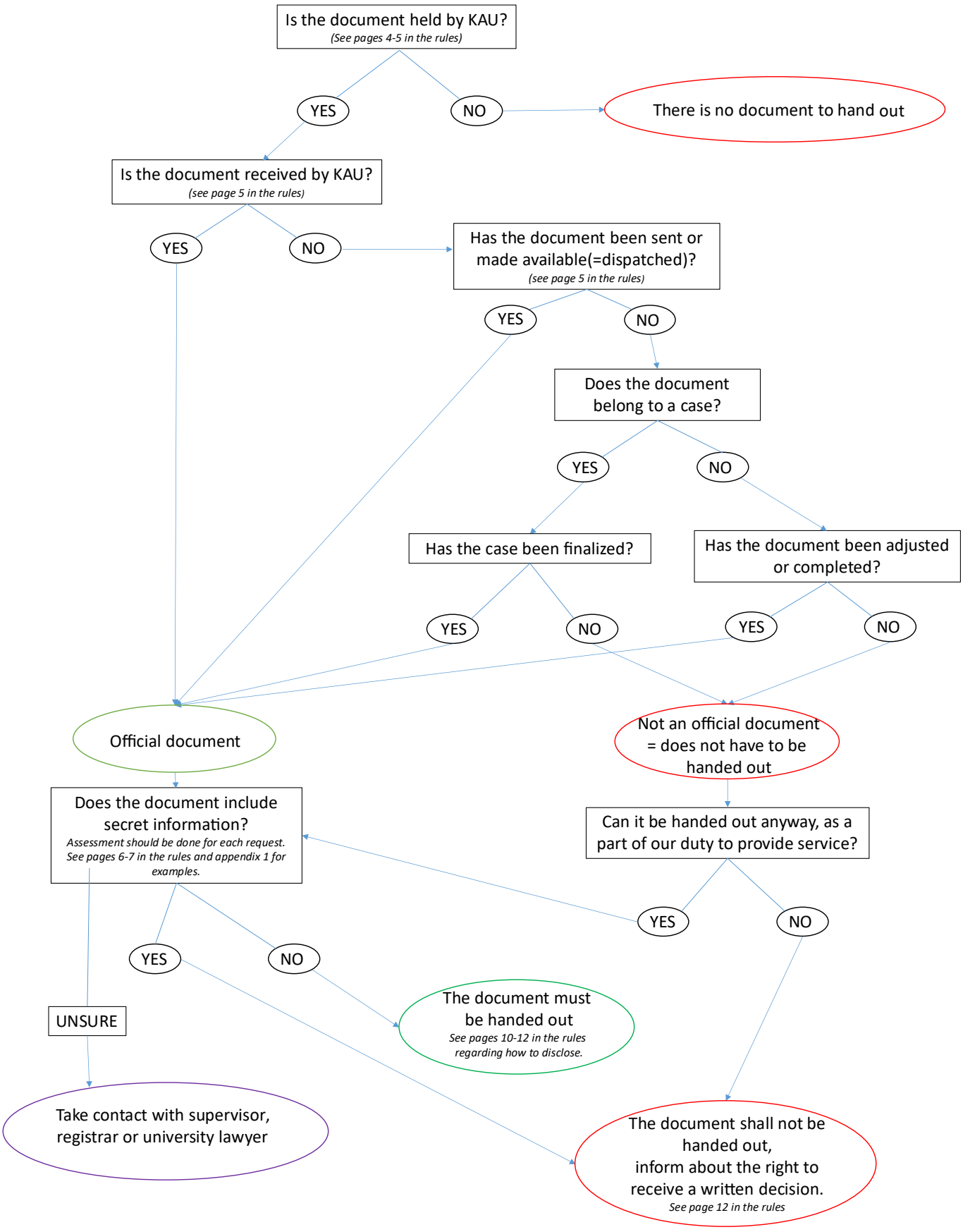
Examples of sections in the Public Access to Information and Secrecy Act concerning universities

Paragraph	Secrecy area
Chapter 17. Section 3c	tests and exams
Chapter 17. 4 §	controls at the Swedish Scholastic Aptitude Test
Chapter 19. 1-5 §§	business activities of the authorities and the study of natural scientific and technological nature for the public good
Chapter 19. 6-8 §§	information prior to labour union negotiations
Chapter 21. 1 §	information about an individual's health or sexuality
Chapter 21. 3 §	information on persecuted individuals
Chapter 21. 5 §	data relating to foreign nationals
Chapter 21. 7 §	in violation of data protection regulations
Chapter 23. 5 §	student's personal relationship with a psychologist, counsellor or study counsellor, individual student's identity if there is a special reason
Chapter 23. 6 §	expulsion from higher education
Chapter 24. 1 §	psychological examination carried out for research purposes
24 chap. 5 §	research collaboration
Chapter 24. 8 §	information about individuals' personal circumstances in certain research studies (read together with Section 7 of the Public Access to Information and Secrecy Ordinance (2009:641))
Chapter 31, Section 12	contract activities, commissioned research
Chapter 39. 1-3 §§	personnel social and administrative activities
Chapter 40, Section 3	library activities

Whether there may be grounds for classifying an official document as confidential or not must be decided on a case-by-case basis. An assessment must always be made on the basis of the conditions provided by the individual case. Consult a university lawyer if there is any ambiguity.

ASSESSMENT WHETHER A DOCUMENT CAN BE HANDED OUT

Appendix 2



Appendix 3

Examples of documents that must be registered

Agreements
Decisions – Vice-Chancellor, Dean, Head of Department, etc.
Delegations
Interim decisions
Interim reports
Dissertations/doctoral degrees/applications
Disciplinary matters
Docentship – applications Surveys
Dismissal
Ethical reviews
Degrees - establishment of
Doctoral education – application
Research documents – applications and decisions on funds, agreements, contracts, reports to funders/financiers, final financial reports, correspondence with funders that are not of obvious minor importance, etc.
Disability, students with – application and decision of funds
Gift and donation letters
Individual study plans
Establishment of positions - calls, applications, reviews and employment decisions Contracts
Syllabi and reading lists
Licentiate degree
Negative decisions in study administrative matters
Policy documents and local regulations
Appropriation Letter
Referrals
Audit reports
Confidential documents, rehab, relocations
Permits
Credit transfer
Education syllabi
Calls
Procurements
Election to the Board and Committees
Operational plans/stories
Warning
Annual report
Cases/views/questions from students etc. (which are of no minor importance)
Appeals