2018-04-23

CHECKLIST FOR NEWCOMERS
AT THE DEPARTMENT OF ONCOLOGY-PATHOLOGY

Requirements for entrance to the department

☐ Reason and type of financing during stay (page 2)
☐ Documents to the Human Resource unit at Z1:00 (page 2)
☐ Closest relative form (page 3)
☐ General information including safety (pages 4-6)
☐ Guidelines on information security (pages 7-8)

Signature

…… ……
Date Charlotte Rolny, Chairman of Work Environment Group

Leave all pages to Charlotte Rolny, CCK:01

2018-04-23

REASON FOR STAY

Name of employee/student: ……

Position: Student, PhD-student, Postdoc, Senior Researcher, Guest Researcher, T/A

Other: ……..

☐ Employed or stipend at Karolinska Institutet ☐ Employed/stipend at Karolinska Hospital

☐ Employed or stipend at Radiumhemmets forskningsfonder / Cancerföreningen

☐ Exchange student; University: ……

☐ Thesis work/project work for undergraduate studies at KI

☐ Thesis work/project work for undergraduate studies at other university ……

☐ Other reason: ……..

For PhD-students and postdoc with own financing state SEK / month: ……

Information regarding insurance coverage during work hours and to/from work

Employment / stay at OnkPat's premises; From …… To……..

…… ……
Signature employee / student Signature PI / group leader

For the Human Resource unit at Z1:00

Leave a copy of the following documents at the HR-unit, e-mail hanna.sillen@ki.se to book a time. *NOTE! This does not include students conducting a project or thesis work for up to 6 months.*

☐ Residence permit if applicable

☐ Civic registration certificate (personbevis) for employment purpose / Passport / Identity card

☐ Copy of form "Closest relative". The original should be kept in the research group and a copy sent to Hanna.

……
Signature Hanna Sillén, administrator HR unit

CLOSEST RELATIVE / NEXT-KIN

PERSON TO CONTACT
IN CASE OF EMERGENCY 2018-04-23

Employee/student

Surname, first name	Nationality
Phone number (home/mobile)	Address

Name of the Group Leader

Surname, first name	Phone number

Information about closest relatives / next-kin

Name of closest relative 1:	(Relation)
Closest relative's phone number: home/work	Closest relative's address and country:
Name of closest relative 2:	(Relation)
Closest relative's phone number: home/work	Closest relative's address and country:

Signature

Date	Signature employee/student

Please keep the original in your research group and hand in a copy to the administration at Z1:00.

2018-04-23

CHECKLIST

Newcomers should go through the checklist together with the group leader or appointed supervisor. All newcomers should familiarize themselves with routines at the department, which is important for safety.

Hand in the completed and signed checklist to Charlotte Rolny, CCK:01.

A personal entrance card (K- badge) will be obtained when the entire introduction is completed and signed (which should be no later than two weeks after arrival).

Group leader's checklist <u>before</u> arrival of the newcomer

☐ Contact in advance Anne Jensen (Z1 level 00, ext. 7979) if the newcomer is an employee/stipend at KI or alternatively,
Gun-Britt Einar (phone number 545 425 52) if the newcomer is employed by Radiumhemmet Research Funds.

☐ Inform your group that a new person is coming and discuss the accessibility to lab and writing space etc.

Group leader/supervisor's checklist <u>after</u> arrival of the newcomer

GENERAL INFORMATION

☐ Entrance card
Contact Sören Lindén on 3rd floor for a temporary entrance card. This is valid for two weeks, until a personal entrance card has been issued.
soren.linden@ki.se or phone number 070-484 1310.

☐ K- badge
Contact Eva-Lena Halvarsson on floor 00 to order a K-badge.
eva-lena.halvarsson@ki.se or phone number 073-870 0420.

☐ Ask the newcomer to contact Anne Jensen (Z1 level 00, ext. 7979) if the newcomer is an employee/stipend at KI, or alternatively,
Gun-Britt Einar (phone number 545 425 52) if the newcomer is employed by Radiumhemmet Research Funds for general information about the employment.

☐ The newcomer needs to perform the KI online course on equal treatment in Ping Pong. Instructions: Click "logga in i Ping Pong" using your KI-ID. In the menu bar, choose "Events/Aktiviteter" -> "Catalogue/Katalog" and search "online course on equal treatment/webbkurs om lika villkor". Click "start" to begin the course.

☐ Introduce the newcomer on the floor and at regular floor meetings.

☐ Show the common facilities: common storage, dressing rooms, toilets, rest rooms, lunch rooms and notice-boards.

- ☐ Contact persons for safety issues and harassments (see the department of Oncology-Pathology´s intranet on work environment)

- ☐ Inform about KI:s environmental and sustainability guidelines

- ☐ Inform about Previa occupational health service. The service may be used by KI employees and scholarship-funded doctoral and post-doctoral students.
  Previa occupational health service
  Staff support – around the clock telephone councelling

- ☐ Documentation of research results.

- ☐ KI:s help desk for foreign visitors: International staff

- ☐ An overview of CCK, KI, Radiumhemmet´s Research Funds and Karolinska University Hospital.

- ☐ When leaving the group check with the group leader/supervisor what to do with files in computers, material in the freezers and clean your desk etc. Return entrance card and keys to Sören Lindén.

LAB/SAFETY

- ☐ Chemical representative at the department.

- ☐ KS security guard, emergency showers, eye showers, emergency phone numbers, emergency exits, first aid supplies, alarm display for -70^{o}C freezers, emergency equipment for chemical spills.

- ☐ Room for liquid nitrogen storage. Contact Sören Lindén for a brief safety instruction if the newcomer will use liquid nitrogen storage.
  soren.linden@ki.se or phone number 070-484 1310.

- ☐ Contact elle.tisater@ki.se or elisabeth.djup@ki.se for a brief instruction about handling dirty dishes and sterilization.

- ☐ Group leader/supervisor is responsible for organizing a demonstration of equipment. Do not use any equipment without prior instructions.

- ☐ Explain how to use fire alarms and fire extinguishers. Show the gathering place in case of evacuation.

- ☐ Inform about local radiation protection regulations (Radiation protection on the Staff portal)

- ☐ Lab coats should always be used in the laboratory. Exchange of lab coats is available on floor 01. Please remember to return your dirty lab coats as we will be charged extra if they are not returned within 90 days.
- ☐ No food or drink is allowed in the lab.
- ☐ The newcomer should read the lab regulations. These can be found on Onc-Pat's intranet on work environment). It is important that the group leader/supervisor gets confirmation that the newcomer has understood the lab regulations.
- ☐ Work Environment Authorities/Arbetsmiljöverkets regulations (AFS) for safety and health plan. Work environment and health on the Staff portal
- ☐ Guidelines on information security (pages 7-8). Read and sign the document.

INTERNAL SERVICE

- ☐ For IT support contact: fixit@ki.se.
- ☐ Inform about your group's ordering and purchasing routines.
- ☐ Eva-Lena Halvarsson distributes keys to the dressing room and safety boxes and takes care of post boxes and postal services.
- ☐ Copying, phone and fax within and outside of Sweden.

SIGNATURES AFTER COMPLETING THE INTRODUCTION

Leave the signed checklist to Charlotte Rolny, CCK:01

Signatures

……	……	……
Date	Supervisor	Printed name
……	……	……
Date	Employee/student	Printed name
……	……	……
Date	Group leader	Printed name

Guidelines on information security at Karolinska Institutet

About Information Security

Anyone who has an active role, i.e. employees, students, contractors/associates and consultants, are responsible for being familiar with and observing the current rules on information security within Karolinska Institutet (KI).

The purpose of this document is to provide a description of the information security requirements that everybody within KI must be aware of in order to contribute to protecting the organisation's sensitive information.

There is more detailed information for certain functions/responsible persons in KI's rules on information security and in its appendices.

Handling sensitive information[1]

When handling sensitive information, you must bear in mind that:

- you may only access sensitive information that you need in order to be able to perform your work
- your access rights are personal and may never be shared with anyone else. You are personally responsible for the activities performed via your login details.
- sensitive information on paper must be locked away when not in use
- sensitive information may only be sent in encrypted form if sent by email
- sensitive information must never be discussed in a public place or where there is a risk that unauthorised persons may gain access to the information. This also applies to calls made by phone or mobile phone.

IT hardware and portable media

When handling IT hardware and portable media, you must bear in mind that:

- KI's hardware is to be used for work-related purposes
- only hardware that is configured in accordance with KI defined standards may be connected to the network
- information saved on the local hard drive on your computer or portable media must always be backed up. When possible, data should be saved in designated places (document management system, network disks, etc.)
- information on computers, mobile phones and on paper must be protected, i.e. such items must not be left unattended
- mobile phones and PDAs must always be protected against unauthorised access by the use of a PIN code or equivalent
- sensitive information must be encrypted if it is stored on portable IT media

6 things to bear in mind!

1. Protect your login details and never pass them on
2. Lock or log out from your computer when you leave it
3. Avoid sending sensitive information by email. If you do, it has to be encrypted!
4. Do not download files or open attachments in emails if you are not sure what they contain
5. Bear in mind the environment you are in, when you are handling and speaking about sensitive information
6. Make sure that your information is backed up, regardless if it is stored on a stationary computer or on portable media. Contact your local IT support for advice.

Use of the Internet

The Internet connection provided by KI is to be used for work-related tasks. Private use is only permitted to a limited extent and as long as it does not affect your work.

It is <u>not</u> permitted to:

- visit websites that contain violence, racism, pornography, criminal activity or other sites that for ethical reasons are judged not to be appropriate[2]
- download files or programs that are not work-related (incl. music or movies)
- connect a computer to the network while it is simultaneously connected to another network.

Use of email

The email system is for work-related tasks. Private use is only permitted to a limited extent and as long as it does not affect your work.

- Sensitive information must always be encrypted when it is sent by email.
- KI email accounts may be closed if there is any suspicion of crime or abuse
- Your email address should only be used in work-related contexts
- It is <u>not</u> permitted to:
  - send or save offensive information such as violence, pornography and discriminatory words or images[2]
  - send or forward spam or chain mail
  - open, send or forward program files that are not work related
  - automatically forward email to an external, unapproved email address
  - quote a private/external email address as contact information on KI's public websites

[1] Sensitive information includes, but is not limited to, information that is or may become classified as confidential according to the Public Access to Information and Secrecy Act

[2] Exceptions to this rule may be granted if the work/research requires this. These exceptions must be approved by the immediate manager..

Use of social media*

The use of social media within KI is primarily based on the organisation's interests, e.g. to quickly reach various target groups.
You should also bear in mind that:

- private use of social media during work hours is only permitted to a limited extent, and as long as it does not affect your work.
- KI's email address may not be used for private login/communication
- sensitive information must never be communicated through social media
- passwords that are used to log into social media must not be the same as passwords used in KI's internal network

Otherwise, the same rules apply as for the use of email. For further information on dealing with social media, see http://internwebben.ki.se/en/social-media-faqs

Telecommuting

When telecommuting, you must bear in mind that:

- remote connections to KI's network are only permitted through approved communication solutions for remote connection
- only hardware that satisfies KI's security requirements may be connected to KI's internal network (does not affect access to online services, e.g. Contempus)
- sensitive information must be stored and handled in a secure manner in accordance with current security requirements
- sensitive information must always be encrypted when stored on movable media such as laptops, USB sticks or mobile phones

Access and user ID

Regarding access and user ID, you must bear in mind that:

- as a user, you are responsible for the handling of information and the activities that take place during the period when you are logged in with your user ID in a system
- your user IDs, passwords and badges are personal and may never be lent to anyone else
- you must immediately submit a report if you suspect that an unauthorised party is aware of your password or if you have lost your badge.

* Social media are interactive communication services on the Internet, such as blogs, Facebook, wikis and comments on articles.

Logging and examining logs

With regard to logging and examining logs, the following applies:

- all use of the Internet is logged
- for all systems that contain sensitive data, logging takes place of all user activities, i.e. everything we do in the system
- the purpose of the logging is to make it possible to make sure that only authorised persons have had access to certain information
- logs are examined on a regular basis

Incident management

Incident reporting is an important element of KI's work with information security. As a user, you must help by:

- reporting incidents that might affect information security as soon as possible
- reporting incidents to the Head of Department or to a person designated by him/her
- also reporting suspicions of incidents

Examples of information security incidents are:

- incorrect, unauthorized or harmful handling of information, which may cause damage to KI
- information that has fallen into wrong hands
- theft of hardware containing information
- hacking
- malware (e.g. virus) or malicious software

We all have a responsibility!

In order to maintain a sufficient level of protection for information and the system environment, we must work together and continuously. Adopted security rules must be applied and observed by everybody with an active role within KI, i.e. all employees, students, contractors/associates and consultants in the organisation.

Information security is primarily based on common sense and good judgement, in which your knowledge and your actions are decisive. All in all, these are important preconditions that contribute to maintaining confidence in our organisation and guaranteeing the information that we are handling.

Any breach of current security rules can result in a loss of access rights to KI's IT systems. This may be decided by the Head of Department in consultation with the Chief Security Officer/the IT Director. More serious cases of abuse or other similar breaches of rules should be reported to the Chief Security Officer for further processing. Any suspicions of criminal activity will be reported to the police.

Karolinska Institutet

Personalstöd – via telefon

0200-21 63 00

- Gäller för alla anställda samt stipendiefinansierade doktorander och postdoktorer på KI.
- För frågor som rör:
  - privatekonomi och juridik.
  - arbetsrelaterade eller privata psykosociala problem/dilemman.
- Tillgängligt dygnet runt (socionom svarar). Specialist ringer upp inom 72 timmar.
- Upp till tre konfidentiella samtal/konsultationer (utöver det initiala samtalet med socionom).
- Även chefsstöd – via samma telefonnummer.
- Tjänsten levereras av Falck Healthcare.

Staff support – telephone counselling

0200-21 63 00

- The staff support includes both work-related and private matters. The service assists with matters concerning, for example, relationship problems, addiction issues, personal crises and questions regarding legal matters (e.g. tenancy agreements) or personal finances.
- The service may be used by KI employees and scholarship-funded doctoral and post-doctoral students.
- The service is available round the clock (a social worker answers your call).
- You are entitled to up to three confidential counselling calls with a specialist per case/situation. The specialist could be a financial/legal counsellor or a psychologist/behaviour scientist.
- Managers may also use the service to request managerial support for situations concerning, for example, working groups.
- This service is provided by Falck Healthcare.

Karolinska Institutet

The service, which replace *Previa Direct*, is available until 30 June 2018. Please remove this poster at that date.