# Employee Monitoring Policy

## Purpose of the policy

Employee monitoring has the capacity to intrude or interfere in the private lives of individuals and it must, therefore, be justified. The UK General Data Protection Regulation (UK GDPR) does not prohibit monitoring of staff, but any monitoring must be carried out in accordance with the Act.

Monitoring can also be a necessary as part of crime or fraud detection and for ensuring that the University estate, facilities, telecommunications and IT systems are used appropriately. Any benefits to the University of monitoring staff must be weighed against any possible adverse impact on our employees.

This policy sets out the University's approach to monitoring staff, the responsibilities of managers with respect to that monitoring and the individual rights of staff**.**

## Scope of the Policy

This policy applies to all staff who are employed by the University of Nottingham, it also applies to Associate staff, contractors and temporary staff.
The policy will be available on the University website.

The policy applies irrespective of work location and is not limited to work that is conducted solely on campus e.g., working from home but this will be very limited in nature e.g., may only apply to IT monitoring and usage.

## Core principles

- Staff have legitimate expectations of privacy within the University.
- Staff monitoring is not a method of performance management and managers who have underperforming staff should use the existing routes of 121's/performance plans and HR advice to resolve those issues.
- Intrusion into the private lives of staff is not justified unless the University is at risk.
- The University should have a clear idea of the benefits that monitoring will bring and must be able to justify these against any adverse impacts on staff.
- Staff must be made aware of the nature, extent and reasons for any monitoring which is likely to take place. The exception to this is when prior notification of the member of staff concerned could lead to the concealment of evidence or would otherwise be likely to compromise an investigation into a very serious disciplinary matter or potential criminal activity. In such cases, an impact assessment will take place prior to any monitoring.
- Staff are expected to abide by the current policies and procedures in place and take responsibility for their own conduct.
- Specific monitoring may be carried out in line with statutory requirements, e.g., monitoring of the Joint Academic Network IT system (JANET).
- Staff should be aware of the University's Code of Practice for users of University Computing Facilities as this details what is acceptable use of IT and communications

facilities. The University will operate in line with RIPA (Regulation of Investigatory Powers Act 2000) but communications are unlikely to be intercepted.
Reminders of these codes will be provided to all employees through normal update channels.

## High Level Definitions

### Monitoring
Activity which sets out to collect information about staff by keeping them under some form of observation and goes beyond one individual simply watching another and involves the manual recording or any automated processing of personal information.

### Systematic monitoring
Where all staff, or groups of staff are monitored as a matter of routine. An example might be to establish patterns of use or demand for a service. This may or may not identify individuals.

### Occasional monitoring
Short term measures in response to a particular problem or need.

### Covert monitoring
Monitoring which is carried out in a manner calculated to ensure those subject to it are unaware it is taking place.
Covert monitoring by the employer should be reserved for cases of likely serious misconduct, where strong evidence or suspicion exists and can be shown, rather than minor offences.
The University will always only undertake such monitoring as a last resort in the most serious of cases, where to reveal monitoring is taking place could lead to the destruction of evidence.

### What is not covered by this policy:
- Audit – auditors monitor systems and processes rather than individuals
- Equal opportunities monitoring.

## Authority for monitoring

Unauthorised staff monitoring is not permitted. Attempts by any member of staff to implement unauthorised monitoring or recording will be in breach of this policy and that activity may result in disciplinary action.

The following is a list of those members of staff, in addition to the Vice Chancellor, Registrar and the Director of Human Resources, who may authorise monitoring together showing their areas of responsibility.

- Head of Security – any physical security matters, e.g., CCTV/Police Requests/Assaults/Sexual Offences/Breaching the law/regulations.

- Chief Financial Officer – any financial matters, e.g., suspected fraud.
- Chief Digital Officer or Chief Information Security Officer – any IT matters, e.g., Internet and e-mail usage or matters related to IT or data security
- Director of Estates and Facilities – any matters relating to the use of the University estate and its facilities.

These individuals may also designate a nominee/s to authorise monitoring on their behalf in line with the schedule of delegated authority for investigations which can be found at the end of this policy at Annex 2.

## What may be monitored and why?

Employee's activity may be monitored as part of an investigation into misconduct, in a staff member's absence or for reasonable University activity i.e., activity that is needed for the safe and effective running of the University.

Monitoring activities can be categorised as:

- Physical
  - Routine use of CCTV to check that health and safety rules are being complied with, to assess if an act of misconduct can be established or to assist in the prevention of crime e.g., theft by acting as a deterrent or capturing evidence of perpetrators.
  - Use of Body worn cameras – as CCTV and also for the safety of security staff.
  - Monitoring Access Control Cards for buildings and individual access e.g., to corroborate staff location where relevant to the investigation.
- Telephones
  - Keeping recordings of telephone calls that come into the University for training purposes or for dealing with complaints.
  - Checking telephone logs to detect misuse of telecommunications.
  - Accessing voicemails during staff member's periods of absence, so that work matters can be picked up, e.g., if phones have not been forwarded.
- E-mails
  - Accessing an email box to place an out of office on and to pick up any relevant work emails during a staff member's period of absence.
  - System filtering for spam e-mails.
  - Requesting an IT search of emails where allegations of serious misconduct are alleged e.g., sexual or racial harassment.
- Internet and IT Equipment
  - Examining website logs to ensure that staff are not visiting inappropriate sites.
  - Examining the contents of computer hard disks to check for any unlicensed software or to see if updates are needed.
  - Accessing other computer logs, data and hardware where allegations of computer misuse or staff misconduct require a disciplinary investigation.
  - Requesting IT searches on information held on UoN systems for the purposes of compliance with a legal obligation such as the duty to preserve document

This provides the majority of monitoring undertaken and any new or additional monitoring will be reflected here and in the University Privacy Notices.
The policy will be subject to annual review.

There are occasions and examples, including those listed above, where monitoring is carried out, but the data collected is only viewed retrospectively to investigate an incident i.e.,

system logs may only new actively viewed following the raising of a suspicion of viewing illegal material.

## Informing staff of monitoring activities

Managers must seek HR advice and guidance before monitoring staff, and any monitoring must be approved by the Authorising Officer using the Employee Monitoring Data Privacy Impact Assessment (Appendix A).
Monitoring staff is not a way of managing staff's performance.
Informal routes such as one to ones, team meetings and setting and managing objectives is the appropriate and effective way in gaining the improvements required.
Where informal performance management has not been successful the manager should seek advice from HR. Monitoring will only be appropriate if the performance becomes a matter of potential misconduct.

Staff must be notified of the nature of any monitoring that is taking place, unless to do so would prejudice any investigation e.g., by tipping off and allowing an individual to destroy evidence.
If any changes are made regarding monitoring, staff will be notified.
The exceptions to this are: covert monitoring activity, e.g., for crime detection, which is allowed for by the Regulation of Investigatory Powers Act (RIPA) 2000 and any successor legislation; and retrospective monitoring in response to allegations raised and formal investigation being conducted.

## Concealed Recording

The University does not permit the concealed recording of meetings by staff of any level, where other members of staff are unaware that they are being recorded.

This is true regardless of whether the meetings are conducted in person, via technology such as Microsoft Teams or by phone. Such secret recording may amount to a breach of privacy and confidence actionable under the University's disciplinary procedures.

## How monitoring information will be used

Any monitoring information that is collected in relation to a member of staff may be used in a disciplinary investigation, for example, where there is inappropriate use of the internet or e-mail.

Monitoring information may be used for training purposes, for example telephone training and staff will be made aware of this.
Information collected may also be passed to relevant authorities if there are any criminal proceedings to which it relates.

## Employee Monitoring Impact Assessments

The ICO Employment Practice Code (Part 3) recommends that in all but the most minor cases, an 'impact assessment' should be carried out by the manager making the request to

decide if and how to use monitoring. This involves measuring the benefits monitoring may bring; any adverse impact on individuals or third parties, whether similar benefits can be achieved with a lesser impact, and the techniques available for carrying out monitoring. A decision will be made as to whether the monitoring is a proportionate response to the individual situation it seeks to address.
The Employee Monitoring Impact Assessment (EMIA) should be provided as part of the document disclosure process for disciplinary and grievances.

The University has implemented an EMIA process in line with this guidance, which can be found at Appendix A.

Please note that this is different to the Data Protection Impact Assessment (DPIA) process as that is related more too large-scale projects/systems and processes.

## Things to consider before monitoring staff members

The consequences of monitoring must be considered in terms of any potentially adverse impact on staff.
Before monitoring takes place guidance from a HR representative may be sought and the Employee Monitoring Data Privacy Impact Assessment should be completed:

- What intrusion will there be into the private lives of staff, e.g., interference with their private telephone calls or e-mails.
- To what extent will staff be aware that they are being monitored?
- What impact, if any, will there be on the relationship of mutual trust and confidence between staff and the University.
- Whether information that is confidential will be seen by those who do not have a legitimate business need to know.

Alternatives to monitoring should be considered, for example:

- Can established or new methods of supervision, training or clear communication deliver acceptable results?
- Can investigations be carried out on specific incidents, rather than monitoring continually?
- Can monitoring be limited to only those staff about whom complaints have been received or who may be suspected of significant wrongdoing?
- Can monitoring be automated? but only where this does not increase the risk of intrusion
- Can monitoring be targeted only to areas of high risk?
- Can audits or spot checks be carried out instead?

The decision as to whether the current or proposed method of monitoring is justified involves:

- Establishing the benefits of the method of monitoring.
- Considering any alternative method of monitoring.
- Weighing benefits against adverse impact.
- Ensuring that any intrusion is no more than absolutely necessary, taking into account the results of consultation with staff or students or their representatives, e.g., trade unions, student union.

## Retention of information

- Impact assessment documentation should be kept for six years after the monitoring has ended.
- Completed impact assessments should be kept within a relevant casefile by the individual completing the form.
- Personal data collected during the monitoring process should only be retained for as long as is necessary to fulfil the purposes of monitoring set out in the impact assessment. It should be securely destroyed once it is no longer needed, in accordance with the University's record retention schedule.

### Individual rights

The DPA 2018 and the GDPR confers on individuals' various rights including the right to find out what information a Data Controller holds about them – the right of subject access. Personal data collected or kept by the University for the purposes of monitoring will be made available if a subject access request is made, unless a legal exemption applies.

**Related UoN Guidance for Staff**

All staff should read and refer to the following documents to make sure they are fully aware of the supporting polices and guidance that cover acceptable use of IT systems, data protection requirements and CCTV.

Relevant policies and procedures can be found on the University website here.
This includes IT policies governing the use of IT and Information Security which can be found here

The UK GDPR sets out the responsibilities of organisations processing personal data and the rights of individuals with respect to the use of their personal data.

Further information on Information Compliance within the University can be found on the website here and the Information Compliance SharePoint site here.

The staff privacy notice can be found here.

For CCTV information please see the CCTV Policy here.

Independent Guidance can be found on the Information Commissioners website

## Appendix A

## Employee Monitoring Impact Assessment for the purposes of Investigations

University of Nottingham
UK | CHINA | MALAYSIA

## 1. Scope

This Employee Monitoring Impact Assessment (EMIA) is a specific assessment to use when monitoring of an individual employee is required. The assessment should be used to record the rationale for and approval of any requests to monitor/access staff electronic communications information covertly (i.e., without the staff member's specific consent) during investigations under relevant University policies such as:

- Fraud Policy Statement and Fraud Response Plan
- Disciplinary policies
- Code of Research Conduct and Research Ethics

The form has been specially designed meet the requirements of the Employee Monitoring Policy and is not to be confused with the project/system-based Data Protection Impact Assessment.
The form is also recommended for approval of any requests to monitor/access student electronic communications information during investigations under the Code of Discipline for Students.

Guidance on assessing the likely intrusiveness of proposals is provided at the end of the form, and this determines the level of authorisation required.

## 2. Details of proposed monitoring/information access requested

| | |
|---|---|
| **Name and role of proposer** | |
| **Case reference number** | |
| **Date** | |
| **What monitoring or information access is proposed? Please detail any search criteria including time periods.**<br>Note: *The approver will use this highlighted section to instruct Information Services* | **The reason for this request** (include details of why you consider the request to be proportionate and why alternatives to the proposed monitoring would not be adequate. Provide details relating to whether staff are aware of the monitoring taking place?) |
| 1. | 1. |
| 2. | **2.** |
| 3. | 3. |
| 4. | 4. |

## 3. Employee Monitoring Impact Assessment (to be completed by the authorising officer)

| | |
|---|---|
| **Are the concerns under investigation sufficiently serious to warrant covert monitoring?** | |

| | |
|---|---|
| **How intrusive is the proposed approach for the individual? (See guidance in Annex 1)** | **Not intrusive** / e.g., System data only<br>**Limited intrusiveness** / e.g., Reports/lists<br>**More intrusive** / e.g., Messages<br>**Highly intrusive** / e.g., Whole mailbox or device |
| **What is the impact, if any on any Third Party? How can this be removed or mitigated?** | |
| **Could less intrusive methods be used instead? If not, explain why.** | |
| **Are any search criteria sufficiently narrow?** | |
| **Have the search criteria been defined in a way that minimises the risk of obtaining Special Category Data?[1]** | |

## 4. Decision (to be completed by the authorising officer)

| | | | |
|---|---|---|---|
| **Name and role of authorising officer considering the request** (See Annex 2 for delegated authorities) | | | |
| **Decision** | **Approved in Full** | **Approved in part or with modifications** | **Rejected** |
| | | | |

[1] Special category data' is personal data revealing: racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data (when used for identification purposes), data concerning health, a person's sex life or their sexual orientation.

| | | | |
|---|---|---|---|
| | | | |
| **Any restrictions or modifications required** | | | |
| **Review Period / Length of authorisation** | | | |
| **Optional notes** | | | |

## 5. Communication and retention of decision

If approved, authoriser to pass the request to IS for action, using the content if the highlighted box in Section 2 above[2], copying in the proposer.
Note IS should not receive the full EMIA.
The EMIA should be retained securely for six years after the monitoring has ended (see Employee Monitoring policy).
Approvals may be subject to Internal Audit checks to ensure they are completed properly, and the monitoring meets the terms of the Employee Monitoring Policy.

[2] Director of Service Delivery, Jason Phoenix; Head of IT Security, Joseph Taylor; and Senior Systems Development Officer, Aidrian Shelton

**Annex 1**
**Employee Monitoring Impact Assessment - Guide to assessing and minimising intrusiveness of monitoring**

| | Not intrusive | Limited intrusiveness | More intrusive | Highly intrusive |
|---|---|---|---|---|
| **Summary** | System data only | Reports/lists | Messages | Whole mailbox or device |
| **Examples of requests in this category** | • Count of emails sent to/from certain addresses/domains within a certain time period.<br>• Placing an account on legal/litigation hold | • Report of messages sent to/from certain addresses within a certain time period.<br>• Report of messages containing certain words/phrases within a certain time period. | • Request for a copy of a specific email/emails.<br>• Blocking emails from certain senders to a certain recipient (with the recipient's permission) | Request for access to a copy of a whole mailbox.<br>Request for access to a device (e.g., computer, phone) provided by the University |
| **Steps to minimise intrusiveness** | Specify time period<br>Data Protection Impact Assessment | • Authoriser to consider whether there are less-intrusive and pragmatic other means of achieving the objective.<br>• Specify time period<br>• Consider whether email subject is required<br>• Data Protection Impact Assessment | • Data Protection Impact Assessment required<br>• Authoriser to consider whether there are less-intrusive and pragmatic other means of achieving the objective.<br>• Do not request unopened messages<br>• Do not request messages that appear to be personal or private.<br>• Stop reading any messages where it becomes apparent that they are personal or | • Data Protection Impact Assessment required<br>• Authoriser to consider whether there are less-intrusive and pragmatic other means of achieving the objective.<br>• Do not read unopened messages<br>• Do not open messages or files that appear to be personal or private.<br>• Stop reading any messages or files where it becomes apparent that |

| | Not intrusive | Limited intrusiveness | More intrusive | Highly intrusive |
|---|---|---|---|---|
| | | | private although this was not previously known.<br>• do not request 'special category data' (other than data that relates to the commission of a criminal offence) unless absolutely necessary.<br>• Configure autoreply to sender of blocked messages advising the message was undelivered. | they are personal or private although this was not previously known.<br>• do not request 'special category data' (other than data that relates to the commission of a criminal offence) unless absolutely necessary.<br>• Minimise timescale of access. |

University of Nottingham
UK | CHINA | MALAYSIA

## Annex 2: Schedule of Delegated Authority for approving Employee Monitoring Impact Assessments

| | Not intrusive | Limited intrusiveness | More intrusive | Highly intrusive |
|---|---|---|---|---|
| **Summary** (See definitions in Annex 1) | System data only | Reports/lists | Messages | Whole mailbox or device |
| **Approval** | One of the following:<br>• Any HR Business Partner<br>• Any member of the Internal Audit Service<br>• General Counsel/Director of Legal Services or Deputy Director of Legal Services<br>• Head of Research Integrity<br>• Director of Research and Innovation<br>• Staff with summary jurisdiction powers Section D 13 Code of discipline for Students (student cases) | One of the following:<br>• Director of Internal Audit<br>• Head of HR Business Partnering, or Director of HR<br>• General Counsel/Director of Legal Services or Deputy Director of Legal Services<br>• Head of Research Integrity<br>• Director of Research and Innovation<br>• Staff with summary jurisdiction powers Section D 13 Code of discipline for Students (student cases) | One of the following:<br>• Director of Internal Audit<br>• Head of HR Business Partnering, or Director of HR<br>• General Counsel/Director of Legal Services or Deputy Director of Legal Services<br>• Director of Research and Innovation<br>Staff with summary jurisdiction powers Section D 13 Code of discipline for Students (student cases) | One of the following:<br>• Registrar<br>• Deputy Vice-Chancellor<br>• Vice-Chancellor<br>• Director of Research and Innovation (for Research Misconduct) |