# Access to Information Guide and Form

| | |
|---|---|
| **Owner:** | Security Architect |
| **Author:** | Norman Hogg |
| **Creation Date:** | October 2017 |
| **Review Date:** | October |

**Document Status:**
Draft

## Scope

This is a high-level guideline and request form for managers to request access to information for investigatory purposes. Please familiarise yourself with the Protective Monitoring Access to Information Procedure (Hyperlink when on Zone) before completion.

- **If you believe the investigation is likely to result in criminal charges then further advice must be sought. If in the process of an investigation this becomes the case the investigation must immediately stop and further advice sought. Failure to do so may prevent such charges being brought.**
- **It is important that only the information necessary to any investigation is requested.**
- **Information obtained or supplied must be treated as OFFICIAL SENSITVE [PERSONAL] and held securely (e.g. password protected) so it cannot be accessed by others.**

- This form is for requesting access to any information Aberdeen City Council collects as part of Protective Monitoring
- All such requests require authorisation by the head of department and an HR advisor. Where the head of department is the requester then the Senior Information Risk Owner (SIRO) must authorise the request. In all cases someone more senior than the requester **must** authorise the request.
- Any request must be justified under the principles of current Data Protection legislation. In summary, they must be:

| | |
|---|---|
| Lawful | Access must be for legitimate and lawful reasons. |
| Justified | There must be reasonable suspicion of wrongdoing, not just a "fishing" exercise. |
| Proportionate | The information requested should be proportionate to the seriousness of the suspected wrongdoing. |
| Necessary | Only information actually required should be requested. Access to information should be the only means available of gathering evidence required for the investigation. |

- Information requested may include:
  - Browsing history (in-depth analysis which may include links clicked within sites, bandwidth usage, files uploaded/downloaded, etc.)
  - Email history (this may include access to logs, access to Emails, etc.)
  - Access history (this may include access to logs, audit trails, etc.)

## Related Policy Document Suite

Policy and Strategy

- ICT Acceptable Use Policy
- Employee Code of Conduct
- Protective Monitoring Policy (Hyperlink when on the Zone)

Procedures

- Access to Information Procedure (Hyperlink when on the Zone)

Assessments

- Protective Monitoring Privacy Impact Assessment (Hyperlink when on the Zone)
- Protective Monitoring Risk Assessment (Hyperlink when on the Zone)

### Related Legislation and Supporting Documents

Acts

- The Data Protection Act (1998)
- General Data Protection Regulation
- The Computer Misuse Act (1990)
- The Copyright, Designs and Patents Act (1988)
- The Health & Safety at Work Act (1974)
- The Human Rights Act (1998)
- The Regulation of Investigatory Powers (Scotland) Act 2000
- Telecommunications (Lawful Business Practices) (Interception of Communications) Regulations 2000 (LBPR).

Standards

- ISO27001/2

- PSN

Regulations

- PCI DSS

Best Practice Guides

- National Cyber Security Centre (NCSC) Good Practice Guide 13 - Protective Monitoring (GPG 13)
- Information Commissioner's Employment Practices Code; Part 3 Monitoring at Work.

# Activity Report Request

| ServiceNow Reference: | |
|---|---|

| | Please tick |
|---|---|
| **Access requested to:** | |
| Browsing history | ☐ |
| Email history | ☐ |
| Access history | ☐ |
| **Other** (please specify) | ☐ |

| **Details of Request** | |
|---|---|
| Name of Accounts Under Investigation | |
| PC/Laptop number | |
| ACC employment status | |
| Reason(s) for Request | |

| Details of Information Requested | |
|---|---|
| Information Required | |
| Period to be reported | |
| Data to be made available to | |
| Request made by | |
| Position | |
| Signed | |
| Date | |

| Authorisation by Head of Service or SIRO | |
|---|---|
| Request | Approved ☐ Denied ☐ |
| Name | |
| Position | |
| Signed | |
| Date | |
| Comments | |

| HR Advisor consulted | |
|---|---|
| Name | |
| Position | |
| Signed | |
| Date | |
| Comments | |

**All authorised forms should be scanned and Emailed back to the sender, delivered by hand or returned in a sealed envelope marked OFFICIAL SENSITIVE [PERSONAL] to:**

**Security Team, IT & Transformation, Business Hub 17, 3rd Floor North, Marischal College, Broad Street, Aberdeen, AB10 1AB**