Reassessment	ANNUALLY

Protective Monitoring
Access to Information Procedure

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

Document Status:
Draft

Scope

What is this procedure for?

This procedure is to be followed for requesting access to any information Aberdeen City Council collects as part of Protective Monitoring. This is a high-level procedure which covers:

- The circumstances under which access to ICT User Accounts and Information may be granted.
- The procedure which must be followed when requesting such access.
- The procedure to be followed by ICT staff to fulfil that access.

Who is this procedure for?

This procedure is of importance to **all staff**. It is particularly important for:

- Anyone who has management responsibilities.
- Anyone who is leading an investigation.
- All ICT staff.

- **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 that it cannot be accessed by others.**

Information Request

A request for information on an employee's browsing, Email or access history may be received from a manager or head of any department, the fraud team or official sources e.g. the police. In all cases a strict process and procedure **must** be followed so that the appropriate audit trail and evidence of authorisation can be maintained.

Any request must be justified under the principles of current Data Protection legislation. In summary:

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 incident being investigated.

Necessary. Only information actually required should be requested. Access to information should be the only way of gathering the evidence for the investigation.

Examples of possible reasons for request:

- Suspected Emailing of confidential information to external or unauthorized addresses.
- As part of an ongoing investigation.
- Suspicion of unlawful activities.
- Suspected breach of the Acceptable Use Policy.

Where the information is being sought in relation to an individual's actions, the individual should wherever possible be informed. A failure to do so may contravene the Data Protection and Human Rights acts and you must therefore liaise with an HR adviser in these situations.

There are specific exemptions within the Data Protection Act 1998 for not informing the individual if it is in relation to 'the prevention or detection of crime'. It is advised again that you must liaise with an HR adviser who will in turn involve the Fraud team and/or Legal and Democratic services colleagues where applicable and appropriate.

Where the Police or other external body requests access to information, specific Data Protection exemptions may also be considered. The Police will send in a completed exemption form, which will be retained for the audit trail. In all cases where an external body requests information this should be handled as a 'Third Party Request for Personal Information'. See Corporate Data Protection Policy

In performance of their duties, ICT security personnel may come across situations of concern regarding an individual. These concerns shall be relayed to the appropriate management or authority. Further analysis must not take place without instruction and approval of said management or authority. In all cases this procedure **must** be followed so that an appropriate audit trail and evidence of authorisation can be maintained.

An information request **must** be authorised by the head of department or their delegated authority. Where the head of department themselves is requesting information then the Senior Information Risk Owner (SIRO) or delegated authority **must** authorise the request. Where the SIRO themselves is requesting information then the Chief Executive or delegated authority must also authorise the request.

In all cases someone more senior than the requester **must** authorise the request.

Information requested may include:

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

Requester Procedure

- When requesting information, the requester must ensure that they are doing so with respect to current Data Protection legislation. If in doubt further advice should be sought from their Head of Department, IT, or Legal team.

- The requester should log a Service Now call either directly or after discussion with an IT Manager or the IT Security Team. This call should contain **minimal** information stating only that it is a request for access to "activity information regarding a member of their team". Details of the person being investigated or the reasons behind the request **should not** be included.

- A Security Team member will send an "Activity Report Request Form" for completion. This form should be completed giving enough detail as to what information is required and why. The form should be authorised by Head of Department, SIRO, or Chief Executive as appropriate and signed by an HR advisor.

- Completed forms should be scanned, hand delivered or sent via internal mail back to the Security team member dealing with the request. If internal mail is used, please ensure it is in a sealed envelope and marked OFFICIAL SENSITIVE [PERSONAL].

- The Security Team member will then acknowledge receipt to the requester and the authoriser and commence with the request.

- It is the responsibility of the requester to handle any information provided with Data Protection in mind. This may include password protecting information or redaction.

ICT Procedure

- A request coming from any source is logged as a call in Service Now under the Security Team. This call should contain minimal information stating only that it is a request for access to "activity information regarding a member of their team". Details of the person being investigated or the reasons behind the request **should not** be included.

- The Security Team will add the Service Now reference number to - and send an "Activity Report Request Form" to the requester. The Security Team will update the Service Now call stating this has been done.

- On return of the form the Security Team shall check that adequate information has been supplied to allow the request to proceed and update the Service Now call. If adequate information has not been supplied advice should be given and the form sent back for completion. Should the Security Team have any concerns regarding the information requested or the reasons for access then they should challenge and seek further authority if deemed necessary. All actions should be referenced in the Service Now call.

- The Security Team **must** ensure that the Head of Service (or their delegate) has authorised the request and that the form has been signed by an HR advisor.

- Should the requestor be the Head of Service then the form **must** be authorised by the SIRO (or their delegate).

- Should the requestor be the SIRO then the form **must** be authorised by the Chief Executive (or their delegate).

- On completion of the paperwork and authorisation the Security Team shall:

    - Scan the form and file the document securely.
    - Send an acknowledgement Email to the requester the authoriser and the HR Advisor acknowledging receipt and approval to proceed with investigation.
    - Fulfil the request.

- The information should be treated as sensitive and the following should apply:

    - Where possible mark all documents with OFFICIAL SENSITIVE [PERSONAL] in the document header or on the title page.

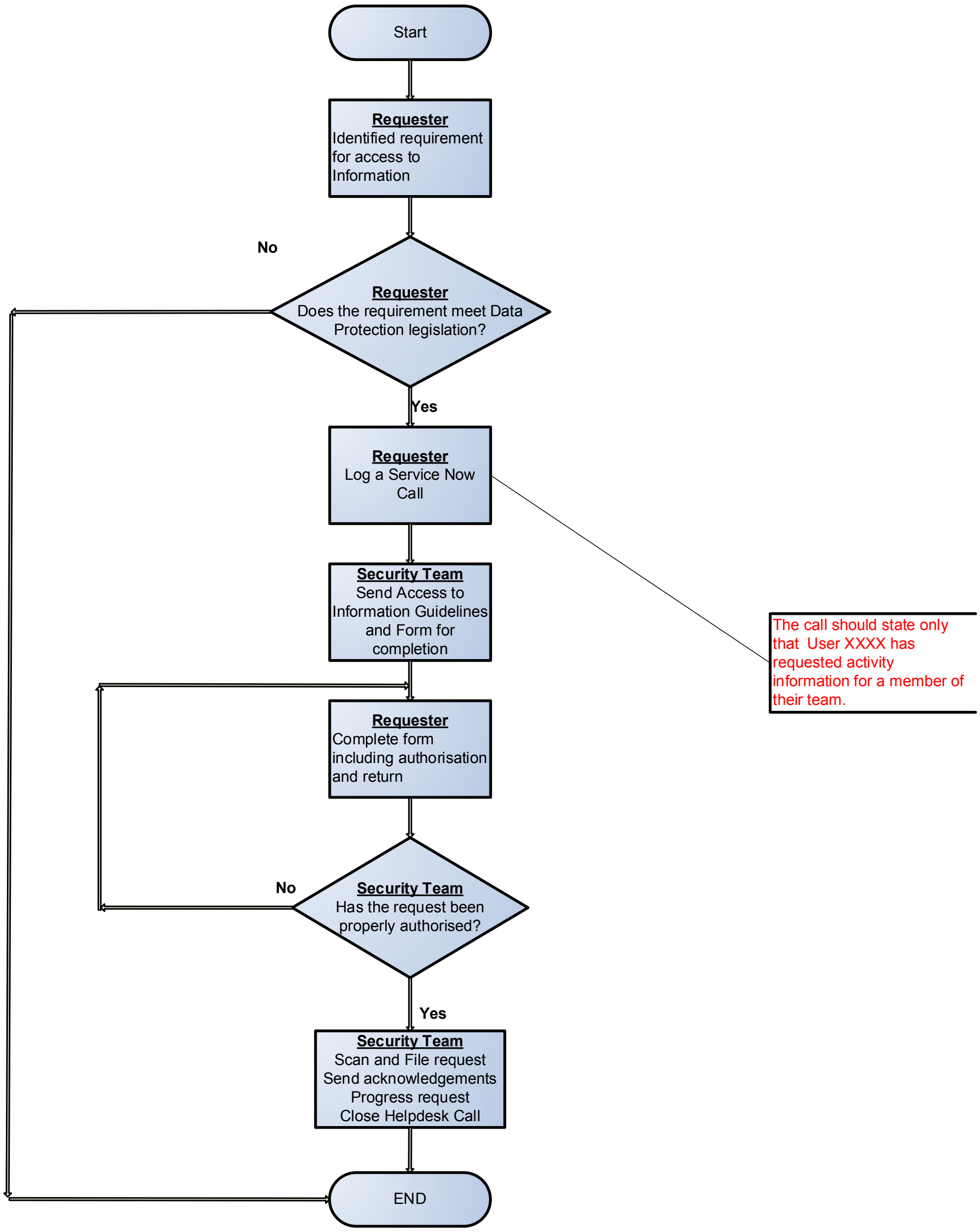
    - Where there are numerous documents, or you are unable to do this the folder containing the documents should have the words OFFICIAL SENSITIVE in the name.

    - Where possible information and documents should be sent password protected or in a password protected Zip file.

- On completion of the Investigation the Security Team should ensure any changes to permissions are reset then update and close the Service Now call.

Access to Information
REQUESTER Workflow

Date Last Updated: 06/10/2017
Review Date: Annually
Process Owner: Security Architect

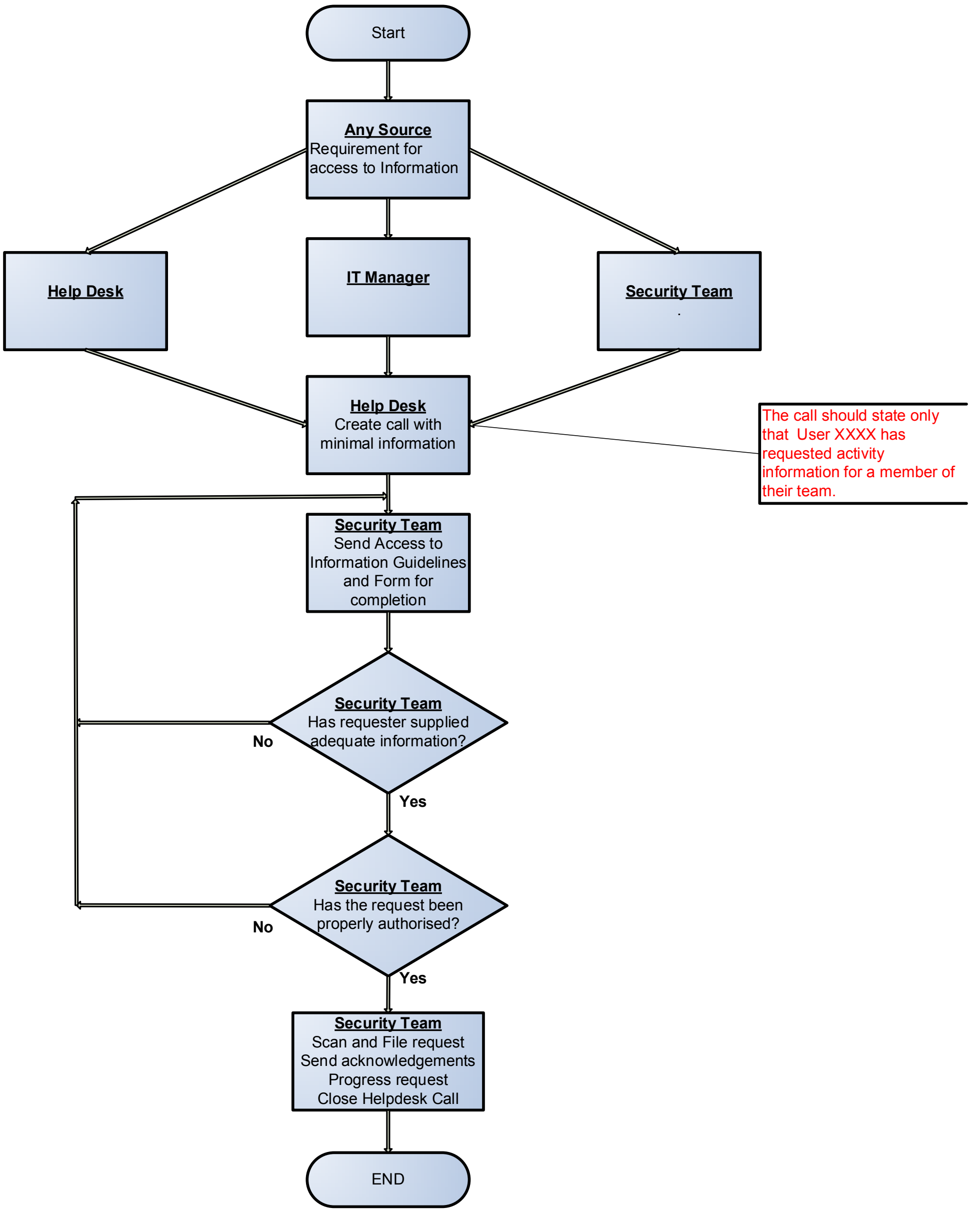


Start
Requester
Identified requirement for access to Information
No
Requester
Does the requirement meet Data Protection legislation?
Yes
Requester
Log a Service Now Call
Security Team
Send Access to Information Guidelines and Form for completion
Requester
Complete form including authorisation and return
No
Security Team
Has the request been properly authorised?
Yes
Security Team
Scan and File request
Send acknowledgements
Progress request
Close Helpdesk Call
END

The call should state only that User XXXX has requested activity information for a member of their team.

Access to Information
ICT Workflow

Date Last Updated: 06/10/2017
Review Date: Annually
Process Owner: Security Architect


Start
Any Source
Requirement for access to Information
Help Desk
IT Manager
Security Team
Help Desk
Create call with minimal information
Security Team
Send Access to Information Guidelines and Form for completion
Security Team
Has requester supplied adequate information?
No
Yes
Security Team
Has the request been properly authorised?
No
Yes
Security Team
Scan and File request
Send acknowledgements
Progress request
Close Helpdesk Call
END

The call should state only that User XXXX has requested activity information for a member of their team.

Related Policy Documents

Policy and Strategy

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

Procedures

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

Forms

- Access to Information Request (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.