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 an 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
- Where request concerns a staff member, all such requests require authorisation by the Chief Officer and an HR advisor. Where the Chief Officer 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.
- Where the request concerns a non-staff member all such requests require authorisation by the Senior Information Risk Owner (SIRO) and the Chief Executive.

- 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 that is actually required should be requested. Access to that 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
- Councillor 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)
  Requires that processing of personal data is done so lawfully and fairly, is used for limited specifically stated purposes and used in way that is adequate, relevant and not excessive.

- General Data Protection Regulation
  From 25th May 2018, this replaces the Data Protection Act (1998) and requires the Council to process personal data lawfully, fairly and transparently, and requires the Council to secure the personal data it holds. The GDPR is designed to enable individuals to better control their personal data. Penalties for breaches are more severe than under the 1998 Act.

- The Computer Misuse Act (1990)
  Disallows unauthorised access or acts in relation to computer systems, data or materials.

- The Copyright, Designs and Patents Act (1988)
  Protects the rights of creators to control the ways in which their materials are used. There is a duty on the Council to prevent breaches of Copyright.

- The Health & Safety at Work Act (1974)
  Protects the health, including mental health of their employees.

- The Human Rights Act (1998)
  The right to respect for family and private life, home and correspondence. This right is not absolute and must be balanced with the need of the Council to protect its information.

- Telecommunications (Lawful Business Practices) (Interception of Communications) Regulations 2000 (LBPR).
  Allows interception of communications by businesses on their own telecommunications networks, for instance, to detect employee-mail abuse or to record telephone conversations to evidence transactions.

Related Standards

- ISO27001/2
  A framework of policies and procedures that includes all legal, physical and technical controls.

- PSN
  A public services shared information and communications infrastructure for which we need to remain compliant.

Regulations

- PCI DSS
  The Council is required to meet this standard in order to take card payments.

Best Practice Guides

- National Cyber Security Centre (NCSC) Good Practice Guide 13 - Protective Monitoring (GPG 13)
  Provides advice on good practice to help meet Protective Monitoring obligations.

- Information Commissioner's Employment Practices Code; Part 3 Monitoring at Work.
  Aims to strike a balance between the legitimate expectations of workers and the legitimate interests of employers.

Activity Report Request

ServiceNow Reference:	

Access requested to:	**Please tick**
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 – what is the trigger for investigation? Access to account information and/or activity requires a justifiable trigger and should not be requested without sufficient probable cause, 'not a fishing expedition'.	
Why do you believe your requested access is legitimate? Do you have reasonable grounds for investigation?	
Explain why access to information is necessary? (are there any other ways of investigating?)	
Explain why access to information is proportionate? (i.e. level of investigation justifies intrusion)	

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

Authorisation by Chief Officer 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