Risk assessment in casework

Risk management in PHSO

1. We recognise that in order to deliver our business programme successfully, and to continue to improve the way this is done, we need to manage effectively the risks which might hamper the achievement of our goals.

2. A risk management framework for PHSO has been developed. The framework defines its approach to risk management, identifies the main reporting procedures and explains the roles and responsibilities of the key players in the risk management process. Within the context of this framework, strategic risks are those that can potentially prevent the achievement of PHSO's overarching medium and long term corporate strategic objectives. Local risk is characterised as those occurring at a Directorate or function level that may prevent the achievement of Directorate key results.

Risk management in casework

3. The monitoring of risk in relation to individual cases is an element of PHSO's risk management framework and it sets out the responsibilities of Directors, Caseworkers and Operational Managers.

4. Case owners have responsibility for assessing risk on individual cases. This includes development and implementation of mitigation plans, updating Visualfiles accordingly and escalating cases via line management as appropriate. (PHSO policy requirement)

5. The intention of this guidance is to:

- ensure that all cases are assessed against consistent risk criteria
- ensure that risk is managed appropriately throughout the life of a case
- to identify high-risk cases early and monitor their progress at an appropriate level

6. Some examples of what might constitute risk elements in casework are: threats to the health and safety of our staff; risk to our reputation; and a risk of litigation. For a detailed list please refer to the Annex A.

When to assess risk

7. The risk assessment of a case (and any linked mitigation plan) should be reviewed regularly throughout the life of a case (for example: in 1:1 meetings or investigation planning meetings) and recorded on Visualfiles. In addition, it should always be assessed at the following stages: (**PHSO policy requirements**)

Assessment cases

- Further Assessment (whether proposal to investigate or decline)

Investigation cases

- Investigation plan agreed
- Draft report issued
- Final report issued
- Compliance plan created

Review cases

- When any 'complaint about us' is received

Assessing and managing risk

8. Case risk is categorised as either **high**, **medium** or **low**

9. Risk assessment is a matter of judgment and it is not generally possible to be prescriptive about the levels of risk that should be applied to particular cases. Consider the following:

- Avoid confusing risk with priority. For example, a high priority case, such as one involving a terminally ill complainant, may be relatively straightforward to deal with.
- When reaching a risk assessment take into account the potential impact of the risk and the likelihood of it occurring. For example, the potential impact of a 'risk to our reputation' might be higher if the risk arises from adverse publicity from an MP. Or, the likelihood of a 'risk of litigation' occurring would be higher if the individual in question had issued proceedings against other bodies. A higher impact and/or a greater probability would normally lead to the risk rating on a case being raised.
- If a case presents multiple risks then the overall risk assessment of the case should represent the highest of those risks.
- If a case presents multiple risks (even if they are low individually) then consider whether those risks have a compound effect sufficient to raise the overall risk rating.
- How the risk can be managed and mitigated. It is not sufficient to simply identify the risk.

10. Where a specific risk has been identified, then the following points should be considered:

- What is the specific nature of the risk in the case?
- What action are we taking to mitigate the risk (provide an up to date mitigation plan)?
- An update on any key issues in the case which may impact upon or change the nature or level of the risk presented?
- Whether the mitigation action fully mitigates the risk or does an unmitigated risk remain (and, if so, should we accept it)?

How to make a risk assessment

11. In order to make a risk assessment on Visualfiles:

- Select 'Edit risk' from the file cover.
- If you are assessing the case as 'medium' or 'high' risk then you must:
  - select at least one of the 'risk categories' (see **Annex A** for full list and examples) by checking the box next to each that applies; and
  - complete a 'mitigation plan' (this is a free text field in which you should record what action needs to be taken in order to manage or reduced the impact or likelihood of the identified risk(s)) (see **Annex A** for examples of mitigating actions relating to specific risk categories). The mitigation plan must describe succinctly the actions to be taken to manage the risk: it should not simply be a description or assessment of the risk.
- If you are assessing the case as 'low' risk then it is not a requirement to select a risk category or detail a mitigation plan. However, that information can be entered if relevant to a low risk case.
- Press the 'Assess risk' button and select either 'high', 'medium' or 'low'.

12. In order to reassess risk on Visualfiles:

- Select 'Edit risk' from the file cover.
- You can then add or remove 'risk categories' or add additional text to the 'mitigation plan'.
- You should also then press the 'reassess risk' button and select either 'high', 'medium' or 'low'.
- If you have added or removed a risk category and/or added to the mitigation plan then you should press the 'reassess risk' button and select the risk level even if the risk level has not changed. This will ensure that the reassessment of risk is logged on the Visualfiles history.

Accessing risk data

13. PHSO risk data can be accessed via the Daily Workload spreadsheet. This can be found in the main reports folder on the I drive.
14. The risk data is contained in columns Y, Z, AA and AB.

15. To search cases by relevant risk categories simply turn on the AutoFilter. This can be done by selecting Data from the top toolbar, then Filters, and then AutoFilter. Once the AutoFilter has been activated, you can then scroll across to the ‘Risk Rating’ column and click on the drop-down arrow to select the level of risk that you wish to confine your search to. For example, choose ‘high’ to view high risk cases.

Annex A: Risk categories, examples and mitigating actions

The table below identifies the risk categories that are available to choose from in Visualfiles. In all circumstances, mitigating action would include notifying immediate line management and addressing the following points:

- What is the specific nature of the risk in the case?
- What action are we taking to mitigate the risk (provide an up to date mitigation plan)?
- An update on any key issues in the case which may impact upon or change the nature or level of the risk presented?
- Whether the mitigation action fully mitigates the risk or does an unmitigated risk remain (and, if so, should we accept it)?

	Risk	Examples/explanation	Other considerations
1	Risk to the safety of our staff	Direct or indirect threats, intimidating correspondence/telephone calls.	Consider use of unacceptable behaviour policy and any other appropriate policies; notify the Security Officer & IT Security Officer

2	Impact on the staff of the body complained about	Safety of staff or damage to an individual's reputation.	Alert body complained about at the earliest appropriate opportunity – but first take advice (from Legal Team or FOI/DPA Team) on whether and how to do this (risk from breach of confidentiality/data protection).
3	Risk to the health and safety of the complainant or others	Sickness, mental health issues, poverty/hardship, wrong medicines. Direct threats, intimidating correspondence/telephone calls. Compliance not being achieved (for example, failure to implement a systemic remedy may be putting patients at risk).	Consider whether release of information to another party is appropriate in order to manager the risk (please refer to guidance on **'Releasing information about risk to a complaint or others'**) Notify the Security Officer & IT Security Officer Seek advice from Outcomes Officer or Compliance Officer in relation to compliance issues.
4	Risk of litigation	Credible threats of judicial review or other legal challenges.	Notify Legal team.
5	Risk to our reputation	Adverse publicity, media interest.	Notify Communications Team and Ombudsman's Casework Manager so that they are aware of potential external interest in the case. (Such a notification does not mitigate the risk and other specific mitigation actions

			should be agreed.)
6	Our approach and/or findings disputed by the body complained about	If the body disputes our findings; or an individual may dispute our findings if we criticise them (for example, an individual clinician or government officer.	Reports should be signed off in line with PHSO **Delegation scheme**. Please note that reports into high risk investigations must be signed off at least at Operations Director level.
7	Previous poor relationship or unaccepted recommendations by the body complained about	If a body has failed to co-operate with previous enquiries or investigations or has refused to accept or to implement recommendations.	Monitor case closely to see if there is likely to be a repeat of earlier dispute. Ensure that information from earlier relevant cases is highlighted and taken into account when formulating draft decision and recommendations. Consider recommending case for referral to the **Recommendations and Outcomes Panel**. Seek advice from Outcomes Officer or Compliance Officer in relation to compliance issues.
8	Risk to our reputation because MP dissatisfied with service/decision	Not just an MP having an interest in the case but only if the MP has or is likely to express dissatisfaction. Not intended for case where we disagree with an MP's presumption of maladministration when	Notify Communications Team and Ombudsman's Casework Manager so that they are aware of potential external interest in the case. (Such a notification does not mitigate the

		referring the complaint to us.	risk and other specific mitigation actions should be agreed.)
9	Unreasonable behaviour by the complainant	Complainant displays abusive, threatening or offensive behaviour Complainant makes frequent, disruptive contact which hinders consideration of their and other complaints	Refer to **unreasonable behaviour** policy and enact via line management Notify the Security Officer & IT Security Officer
10	Sensitive case content	An investigation that featured the Finsbury Park Mosque. Although the complaint was of no particular risk, the Mosque had been at the centre of recent news coverage. A health case where the President of a Royal College was being investigated.	This will depend of course on the nature of the cases but you should seek advice as appropriate from, for example, Communications Team, Ombudsman's Casework Manager, Legal Team, FOI/DPA Team, clinical advisers.

11	Potential conflict of interest	Membership of certain groups, political activities, acceptance of hospitality/gifts; or relationships at work. A conflict of interest may arise from an employee's own interests or activities or from that of a member of their family or an individual with whom they have a close personal relationship. Applies to any member of the Office including the Ombudsman, Advisory Board Members, those on casual contracts, fixed term appointments, Associate Investigators and External Reviewers.	Refer to the **Conflict of interests policy** for advice. Ring-fence conflicted member of staff at early stage.
12	Other	Uncovering possible fraud	Refer to **Fraud policy** for advice

Table: Risk catagories in Visualfiles