Assessing risk in casework

Introduction

1. We need to identify and manage risk continuously through the life of a case, in order to carry out casework effectively and safely. Everyone is responsible for ensuring that risk is managed appropriately.

2. Much of PHSO work is not high risk – most identified risks have potentially low impact and are unlikely to occur. However, given that we cannot anticipate every eventuality, it is vital that we are diligent in our assessment of risk and can evidence a risk based consideration of the information of which we are aware. We need to mitigate any risk identified to the best of our ability.

PHSO's four principles in operational risk management

3. These principles underpin our approach to casework risk assessment. We should:

- **Acknowledge that risk is inherent in the work that we do**
- **Accept no unnecessary risk**
- **Anticipate and manage risk by planning**
- **Make risk decisions at the right level**

Summary

4. There are eight risk categories (see 'risk category definition' below) to consider at key stages of the casework process in relation to likelihood and impact. The categories provide a broad framework for any particular risks identified. Visualfiles must be updated with the most current risk assessment. It is important to know when and how to escalate matters quickly if an immediate risk is identified.

When to do a risk assessment

5. Although risk management is a continuous process, a formal risk assessment is required at four points in the casework process:

a) When we propose to investigate/decline to investigate (case assessment)
b) When we confirm the investigation (under investigation)
c) When we share the draft decision
d) When we decide to do further work following a complaint about our service, decision or method

How to assess risk

6. The following questions must be considered in relation to the risk categories (defined below):

a) Is there a risk? (If so describe the risk in a short statement)
b) What is the likelihood of the risk? (high/medium/low)
c) What is the potential impact? (high/medium/low)
d) How can we mitigate the risk?
e) What do you expect the risk rating to be having taken mitigating action?
f) What action do we take if the risk described at a) happens?

7. Potential action to mitigate risk will significantly vary from case to case (and a discussion with colleagues or a manager might help to clarify your thinking), however action in risk mitigation plans should aim to achieve one of two outcomes:

- Reduction (take action to decrease, or eliminate the likelihood or the impact)
- Retention (accept that the risk cannot be mitigated and is outside PHSO control)

Recording the risk assessment on Visualfiles

8. A risk assessment should be completed on Visualfiles by pressing the 'Edit Risk' button (on the file cover) which takes you to the risk details screen. Select one or multiple categories that reflect the type of risk identified. Where applicable, then complete the following prompts within the mitigation plan field:

1. **Describe the risk** (give reasons for category selection)**:**
2. **Likelihood? L/M/H**
3. **Impact? L/M/H**
4. **Escalation required?**
5. **Plan to reduce likelihood and impact:**
6. **Expected risk rating if mitigating action taken:**
7. **Action to take should the risk described occur:**

NB: remember that a range of people may need to read and act on the information that you supply in the plan, so please be thorough and briefly explain background context if needed. This should include details of third party involvement or interest from other organisations (CQC etc.)

9. The '(Re)assess risk' button should then be pressed to select the overall risk rating (Low, Medium or High) that best reflects the **current** risk. The lowest rating element should be reflected in the overall rating, for example:

- for a risk with High likelihood and High impact, please select High

- for any combination of Medium and High, please select Medium
- for any combination of Medium and Low, please select Low

10. The date will be automatically updated.

Responsibility for high risk cases and dealing with immediate risk

11. Case risk should be managed by the individual allocated ownership of the case.

12. High risk cases are the responsibility of the relevant Director. These cases are monitored at a monthly meeting of senior staff from across the office.

13. If the caseworker identifies a high risk case, this must be discussed with their line manager or Assistant Director as soon as possible. If the manager agrees with the risk rating they should escalate the case to a Director to agree the mitigation plan. Please consider who else may need to be made aware of the case (and involved in mitigation planning), for instance colleagues in External Affairs (parliamentary/health policy staff, stakeholder liaison, the press team); or the Ombudsman's Casework Team.

14. If there is an immediate risk, particularly to the welfare of individuals, it must be considered quickly and a decision taken on what action to take. Please refer to our policies and guidance on unreasonable behaviour and risks to staff which are available here:

- Unreasonable behaviour policy (includes information about risks to staff)
- Disclosing information about risk to a complainant or others

Risk category definitions

15. Assessing these categories should prompt us to consider some of the most common aspects of risk:

1. **Risk to physical and/or mental well-being of staff**
   This includes anything which could cause harm or unwarranted stress to PHSO staff. For example:

   - Explicit or indirect threat of injury or harm
   - History of threats to staff during this or previous complaints
   - Inappropriate or abusive use of social media
   - Unacceptable behaviour towards staff (such as abuse or verbal attacks)

   Please refer to the unreasonable behaviour policy for further advice.

2. **Risk to professional standing of staff**
   For instance, the threat by a complainant or body to refer a person employed by or contracted to PHSO to their professional regulator. This might apply to clinical or legal members of staff.

3. **Risk to complainant, stakeholders and third parties**
   Examples include:

   - Explicit threat of suicide or self-harm
   - History of suicide attempts or self-harm made evident during this or previous complaints
   - Threat of harm to others (such as threats to staff at the body in jurisdiction)

- Potential harm to vulnerable people (such as children, people with disabilities, vulnerable adults or people who require/might require safeguarding)
- Potential impact of revealing previously unknown information (such as unexpected finding of avoidable death)
- A need to maintain complainant anonymity because of third party threats
- Complainant is a whistle-blower
- Personal impact on people or organisations who are not party to the complaint (such as the effect of disclosing the actions of an ex-partner on a Child Support Agency or Cafcass case where there is evidence of an already difficult relationship).
- Potential harm to individual professionals (such as 'named' officers and clinicians) from our activities or findings

Please refer to the policy on disclosing information about risk to a complainant or others for further advice.

4. Risks associated with the wider potential impact of our decision

Please check resources such as Horizon Scanning and the Press Cuttings which can be found on Ombudsnet.

Examples include:

- Complaint relates to issues which we have identified as strategic or systemic and so may have a significant impact externally
- Complaint relates to previous publications where we have already publicly stated a view on an issue
- The complaint is novel (and may be the first of many, and so set a precedent, such as the first complaint about universal credits)
- Casework themes and issues that have been flagged as being of interest or have a context that requires attention
- The complaint has a finding of avoidable death

5. Risks to our ability to carry out our function

Examples include:

- Potential or actual publicity could impact on our ability to investigate in private
- We do not get the cooperation we need from a body or complainant
- Significant challenge to draft report findings and/or recommendations
- Required expertise is rare or unavailable – an example of this would be the Edwards Syndrome case where only two people in the country had knowledge and we could use neither
- Investigating the complaint may pose significant challenges to our resources, capacity and/or costs – an example of this might be an enormous case like Equitable Life
- Investigation requires sensitive documents to be sought or where we are unable to release information due to sensitive nature etc.
- We are required to change approach or process as a result of statutory change via JR/Litigation – an example of this might be Redmond

6. Risks associated with customer experience

For cases where there have been former or ongoing issues with the quality of PHSO service or product. Examples include:

- an upheld review has recommended reopening the case
- the robustness of a previous decision has been successfully challenged, which has undermined confidence in our process
- potential negative publicity is anticipated (please contact …)
- Significant delays in progressing a case, causing negative impact for customer

7. Other

Please note that the categories are not a checklist; nor will they be comprehensive. A category of 'other' is therefore included for any risk factor not captured elsewhere. It is important that any risk is identified, and managed, regardless of category.

8. None identified

If you have fully considered risk in relation to the information available and decide that no risk is currently present, please select this category.

FAQs

When should I complete a risk Assessment?

A prompt will appear when a case is 'Ready for Assessment' asking the case owner to consider if a risk assessment is needed. This is not required on every case. A risk assessment, however, must be carried out when a case is subsequently accepted/declined for investigation (including when Customer Services obtain a Resolution). Risk assessment is an ongoing element of case management and should be updated as appropriate to the evidence/information obtained, especially during the course of an investigation. It therefore lies within the case owner's discretion how frequently the risk assessment is updated.

However, it must be carried out when the investigation is confirmed, and prior to issuing the draft report.

An assessment must also be completed when we decide to do further work following a complaint about our service, decision or method.

Why do I need to do a risk assessment?

Risk assessment and mitigation is necessary in the interests of staff, customers, third parties, organisations or individuals who are complained about, and the corporate body of PHSO.

Management of risk in 'High risk' cases is monitored and discussed at a senior level. It is important that the mitigation plan addresses all of the prompts on Visualfiles. The 'Expected risk rating if action taken' is a useful forecast of how the case might proceed. (It is the current risk, not expected risk that should then be selected via the 'reassess risk' button below the mitigation plan.)

Do I need to complete this process every time?

Much of PHSO's work is not high risk – most identified risks have potentially low impact and are unlikely to occur.

However, given that PHSO staff cannot anticipate every eventuality, it is vital that we are diligent in our assessment of risk and can evidence a risk based consideration of the information of which we are aware. We should be able to demonstrate that we took action to mitigate risk to the best of our ability.

When should I use the category 'risks associated with customer experience'?

We sometimes need to do further work on a case, or begin our process afresh, in light of feedback when a complaint about us has been upheld, or decisions made by senior staff. In these cases, where our previous customer service has fallen short, we might anticipate dissatisfaction from the complainant that needs to be carefully managed. The case may need to be escalated, and monitored more closely than normal.

Initially all of these cases are rated as high risk. However, the Customer Experience category (if applied correctly)will enable us to identify them, and once further work is underway they can be risk rated in light of the individual circumstances of the case and not automatically kept high.

How do I record concerns about our reputation?

Sometimes we need to assess potential adverse publicity on a case, including any impact on PHSO. We have moved away from highlighting 'reputational risk', however, there may be cases where we anticipate negative publicity and this can now be captured under the new category of 'risks associated with customer experience'. This does not mean that we anticipate providing a low quality of service, but that we are aware of potential negative media portrayal that needs to be mitigated robustly, just as with any other risk. For media and press related issues please contact: press@ombudsman.org.uk

Why is there a category for 'Other' risk?

This method of assessing risk is different to that utilised in the past – the 'Other' category is included in recognition that the risk categories outlined do not cover every circumstance.

If you believe that the case represents a risk that is not reflected in the categories presented it should be captured in 'Other'.

Why is there a category for 'None identified'?

This category is to help us evidence that we take a risk based approach to casework. In some cases, following consideration of all the available information there will be no risk factors identified. This category should then be selected and a 'low' rating recorded. The mitigation plan field does not need to be completed.

For reporting purposes we will be able to then distinguish between 'low' risk cases that do have potential elements of risk and a mitigation plan, and those with no risk to manage.

What changes have been made to Visualfiles?

The new categories replace the former selection on the 'edit risk' screen.

For open cases, the existing mitigation plan remains visible and needs to be re-written using the new mitigation plan format (by inserting the headings set out in paragraph 8 of the guidance) when next assessed.

There is a choice of Low, Medium or High at the end of the assessment and the date is recorded automatically.

We intend our future case management system to be more sophisticated at capturing risk.

What if there is more than one type of risk?

The risk categories are not exclusive – if there is more than one aspect of risk reflected in the case then multiple categories can be selected on Visualfiles and addressed together in the mitigation plan. Discussing the categories and mitigation plan with a colleague or manager might help to clarify matters.

If you have any queries or feedback please contact:

[redacted] ([redacted]ombudsman.org.uk in the Operational Improvement Team.

Disclosing information about risk to a complainant or others

Introduction

1. This guidance explains what to do if you think it is necessary to disclose information about risk (that is, the probability of harm being caused) to a complainant or others (this includes, for example, children or vulnerable adults who may be at risk).

2. The guidance covers two main situations:

   - We receive information which indicates that a complainant or someone else is at risk (or is likely to be put at risk) and we need to consider a prompt disclosure in reaction to this information. Examples include a complainant threatening suicide or making a threat against others over the telephone.

   - Our knowledge of the complainant's circumstances means that we make a proactive assessment that there may be a risk to a complainant or others. For example, a risk may arise when we send a decision not to investigate to a complainant with a history of self-harm, or a complainant might threaten to harm their GP if we do not investigate their complaint.

3. Disclosing information (in relation to a health case) that may indicate a potential threat to the health and safety of patients[1] is a separate consideration.

4. We have powers to share decision letters or investigation reports in health cases with other people who we think appropriate.[2] It is unlikely that we will use those powers to disclose information about the types of risks referred to in this guidance. This is because we are unlikely to share whole decisions to alert other parties to such risks and the specific type of information we want to disclose is unlikely to be included in the decision letter or report.

5. Please note that the unreasonable behaviour policy covers the management of threats made to PHSO staff.

6. Any action taken under this policy should be fully recorded on Visualfiles for our audit trail. The Visualfiles entry should include, for example, the exact information we were

[1] *Health Service Commissioners Act 1993* (the 1993 Act), section 15(1) (e). It is also a data protection consideration: *Data Protection Act 1998* (DPA), Schedule 3, Condition 3 (a).
[2] 1993 Act, section 14 (2I).

given, the advice we followed when we decided how to act and the action we took as a consequence. It may be necessary to record these details after the event because of the immediate nature of some threats.

7. If necessary, contact the head of information and records management and/or the head of FOI/DPA for advice about disclosures under this policy.

Identifying risks

8. Information about risks may come from different sources, including telephone calls, emails, letters, social media and medical records. You should only consider disclosing information in the most serious circumstances. Some of the key points to think about[3] are:

- Is there a realistic threat to the complainant or others? (It is not necessary to prove that the threat is valid, but we must be able to show that there are sufficient grounds for concern. A discussion with your manager may be helpful when you assess the threat.)

- Does the complainant have past history which suggests that they are likely to be at risk or be a risk to others? (Although a past history of, for example, suicide attempts may put an individual at greater risk; the absence of past history does not mean that the risk is diminished.)

- Do we have clinical evidence which indicates that the complainant is likely to be at risk or be a risk to others?

- Can we identify an appropriate individual or organisation to disclose the information to in order to mitigate the risk? This must be considered case by case, but options might include disclosure to a GP or other health professional, social services or the emergency services.

- Can we limit the disclosure of information to specific parties (and can we limit the amount of information we need to share)?

- Is the risk of disclosure outside our statutory powers outweighed by the risk to the complainant (or other individuals) and the risk to us if we do not act?

- Is the risk of disclosure in order to protect the vital interests (for example, a life or death situation) of the complainant or other persons? (DPA, Schedule 3, Condition 3 (a), (b))

Telephone calls

9. All threats of harm must be taken seriously. If a conversation with a complainant suggests there is a risk that they will self-harm, attempt suicide or endanger someone

[3] Note: these are only considerations, it is not a requirement to answer 'yes' to all of these to proceed with disclosure.

else, they should, if appropriate, be encouraged first to contact the emergency services or other health or personal support. If the complainant is able to confirm in a calm and rational manner that they will follow the agreed steps and maintain their own safety, then it may be appropriate for us not to take any further action (beyond noting details of the call).

10. If we think that the risk is serious but not immediate, we should explain our concerns to the caller, try to obtain relevant information (for example, their location) and, if appropriate, seek their permission to disclose the information. Ideally, we will agree a course of action with the caller but there may be occasions where we act without the caller's agreement.[4]

11. If the caller reveals that they have already taken self-harm action, for example, they have taken an overdose or cut themselves badly, or if they are in a position of danger where self-harm could be take place or they may be about to harm others, we should consider an urgent disclosure. If appropriate, we should seek their permission to disclose the information and we should also, if it is safe to do so, tell them that we are going to disclose the information and why. If we do not have consent, or if the caller has refused consent for the disclosure, we may still take a reasonable decision to disclose the information in a potential 'life or death' situation.[5]

12. If a caller ends the call before we can get or give all the relevant information, then a judgment will have to be made, on the information available, about whether we need to take any action.

Process: disclosure following reactive assessment of risk

13. This would normally happen when we receive information which shows that a complainant or others are at immediate risk (or are likely to be put at immediate risk) and we need to consider a prompt disclosure in reaction to that information. An example of this is if we receive a telephone call from a person who says that they have taken an overdose or during which they make a specific threat against another individual.

14. Record all stages (including analysis, discussions, decisions and any disclosure) as fully as possible (on Visualfiles if it relates to a case). However, in cases of urgent disclosure, it may be necessary to do this after the event.

- The relevant member of staff (this will normally be the case owner, but there will be circumstances in which other members of staff without knowledge of the case will be involved because they have received the contact in question) should consider the risk to the complainant or others (using the questions in paragraph 8 as a guide). Any case risk assessment should be reviewed on Visualfiles (after the event if necessary).

- Discuss the case with a manager as soon as possible to assess how credible the threat is and to agree the next steps. If the threat comes from an individual with a

[4] DPA, Schedule 3, Condition 3 (a), (b) permits this.
[5] DPA, Schedule 3, Condition 3 (a), (b) permits the sharing of sensitive personal data without consent.

diagnosed mental health history, our normal approach should be to disclose information to their clinician (disclosure to other parties should be considered as appropriate). We do not have to seek legal or clinical advice, but if it is needed, it should be sought at this stage. Inform the security officer of any threats to our staff, property or information.

- If we are to go ahead with the proposed disclosure, an operations assistant director (or above) should be contacted to approve it. If you cannot contact an assistant director quickly, an E1 manager can, exceptionally, approve the disclosure. This approval will include agreeing the organisation(s) to which we are disclosing the information. In the most urgent cases, the disclosure is likely to be to the emergency services. But in appropriate cases we may additionally consider contacting other people/services, such as a mental health crisis team, social/support worker, GP and so forth.

- We can make a disclosure after a verbal authorisation. This should be confirmed later, for example, by email or by a note on the case record.

- It is extremely unlikely that a member of staff will have to act alone when considering or making these disclosures but, if there is a serious and immediate threat to an individual (for example, a telephone call from a person saying that they have taken an overdose) and if an assistant director or E1 manager cannot be contacted immediately, a member of staff may make the disclosure without prior authorisation. In these circumstances, the staff member should notify an assistant director afterwards and record relevant information about the disclosure on Visualfiles.

- We should disclose the minimum amount of factual information needed to mitigate the risk to the minimum number of organisations.

- If possible, the member of staff who identified the risk will make the disclosure by telephone. When they make the disclosure, they should be prepared to answer detailed questions about, for example, the complainant's emotional state or tone of voice.

- When we speak to the recipient, we should tell them that we are giving confidential information for the sole purpose of mitigating the risk in question. If possible/appropriate, we should:

    - Ask them to keep the information secure and only use it for the intended purpose.
    - Ask the organisation to let us know if it tells the complainant that the information that initiated its action came from PHSO.

  (These additional steps may not always be appropriate. For example, we might not mention the security of the information if we speak to the emergency services.)

- Making a telephone disclosure can take some time. If we get authorisation to disclose the information late in the working day, the member of staff concerned may need to stay in the office beyond their usual office hours. If the employee is

unable to remain at work to complete an urgent disclosure, the manager should make the disclosure or ensure that another member of staff has all the information necessary to make the disclosure. Managers should, as far as is possible, make sure that no one is left in the office by themselves while making the disclosure.

- If the disclosure relates to a specific case, the case risk should be reviewed after a disclosure. Please refer to the '*Assessing risk in casework*' guidance.

Process: disclosure following proactive assessment of risk

15. This would normally happen if, as part of our consideration of a case, we take a proactive view that we need to disclose information because of a risk to the complainant or others. This is likely to be linked to the content or outcome of a decision, investigation report (draft or final), or review request, or could be in response to an information request that we think might put the complainant or others at risk. Risk may arise, for example, when we send an adverse decision to a vulnerable complainant or if a complainant has threatened self-harm if we do not uphold their complaint.

16. Record all stages (including analysis, discussions, decisions and any disclosure) as fully as possible on Visualfiles.

- The relevant member of staff (normally the case owner) should consider the risk to the complainant (using the questions in paragraph 8 as a guide) and record an analysis. Any existing case risk assessment should be reviewed.

- The case owner should discuss the case with an available manager to assess the credibility of the threat and agree what steps to take. If the threat comes from an individual with a known mental health history, our normal approach should be to disclose information to their clinician (disclosure to other parties should be considered as appropriate). It is not a requirement in law to seek legal or clinical advice but if it is needed, then it should be sought at this stage. Threats to PHSO staff, property or information should also be relayed to the security officer.

- If we are to proceed with the proposed disclosure, an operations assistant director should approve the proposed disclosure. If no director or assistant director is available, an E1 manager can, exceptionally, approve the disclosure. This approval will include agreeing the organisation(s) to which we are disclosing the information (for example, the police, mental health crisis team, social/support worker, GP, other emergency services and so forth).

- We can make a disclosure after verbal authorisation if necessary, and confirm this later (for example, by email or by adding a note to the case record).

- Give the minimum number of organisations the minimum amount of factual information necessary to mitigate the risk.

- We can make a disclosure by telephone or in writing. If we use email, we should take steps to ensure that the recipient will read it promptly (for example, by asking

them to confirm receipt or alerting them by phone to the information that we are sending). We should also follow the requirements of the protective marking scheme (for example, emailing a secure account where one is available or password protecting documents sent to non-secure accounts).

- The staff member making the disclosure should tell the recipient that we are giving confidential information for the sole purpose of mitigating the risk in question. If possible/appropriate, we should:
    - ask the recipient to keep it secure and only use it for the intended purpose; and
    - ask the organisation to let us know if it tells the complainant that the information that initiated its action came from us.

- It can take time to make a telephone disclosure. If we get authorisation to disclose the information late in the working day, the employee concerned may need to stay in the office beyond their usual office hours. If the employee is unable to remain at work to make an urgent disclosure, the manager should ensure that they, or another member of staff, have all the information necessary to make the disclosure. Managers should ensure that no one is left in the office by themselves while making the disclosure.

- If the disclosure relates to a specific case, then the case risk should be reviewed after a disclosure. Please refer to the '*Assessing risk in casework*' guidance.

Support for staff

17. As soon as possible after the disclosure, the line manager of the member of staff involved (the person who received the information and/or made the disclosure) should meet them to discuss the incident, to talk through their feelings and to raise any concerns or anxieties. The manager and the staff member should also use this meeting to identify any learning about how we handled the disclosure and to decide if there are any lessons to be learnt for the future. If the manager identifies wider learning, they should inform the quality insight team.

18. The manager should also agree an action plan for how staff should deal with further contact with the complainant concerned.

19. Managers and staff involved in these disclosures should also consider whether using the counselling and support services available from the employee assistance programme would be of benefit.

20. PHSO will fully support members of staff who make authorised disclosures in line with this guidance if there is a subsequent complaint about a breach of data protection or our own legislation.

Annex A Legal background: maintaining confidentiality in our casework

- We must act in accordance with the law relating to data protection and freedom of information[6] including maintaining confidentiality of the parties to the complaint and avoiding sharing any information at a time or in a way that may influence or prejudice our work.

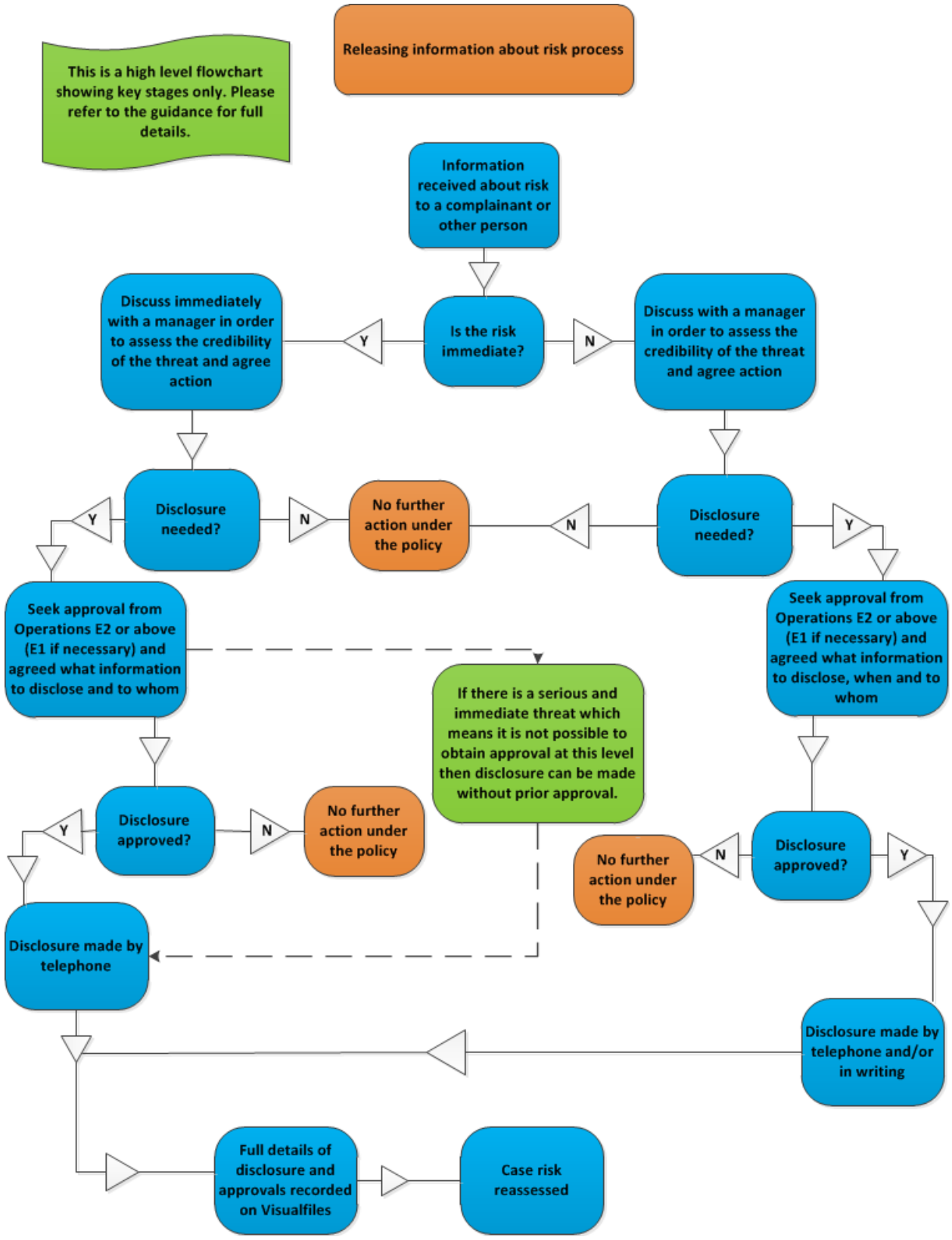
- Our legislation requires that we conduct investigations[7] in private.[8] We should make sure that we maintain confidentiality when we conduct an investigation and are aware of information that is, and is not, appropriate to share between the parties to the complaint. We may disclose information to the parties to the complaint or to third parties where doing so is for the purposes of the investigation or the report and for other limited reasons.[9]

- We should be aware of our responsibilities under the *Data Protection Act 1998* (the DPA) to process personal data lawfully and fairly. We should only share personal information if doing so is necessary for the exercise of our statutory functions. The DPA allows the release of information without the consent of the data subject where doing so is necessary to protect the vital (that is, life or death) interests of the data subject or others.[10]

- Although the release of information in the circumstances set out in this guidance is likely to be a fair and lawful disclosure under the DPA, it may fall outside the scope of our legislation and be a technical breach of our own statutory bar.

[6] *Data Protection Act 1998*. *Freedom of Information Act 2000*.
[7] Please note that these restrictions on the disclosure of information cover all of our casework, including assessment and review work.
[8] 1967 Act section 7(2). 1993 Act section 11(2).
[9] 1967 Act section 11. 1993 Act section 15.
[10] 1998 Act, Schedule 3, paragraph 3(a) (i)-(ii) and 3(b).

Annex B Process flow chart



Quality & Service Integrity > FAQs

Menu

FAQs

Category Disclosing information about risk to others

Questions

1 Do we have a named person within PHSO responsible for child protection who we can discuss any child protection concerns we may have when disclosing information about risk?

2 It would be helpful to have a list of all E2s and their contact details alongside the Disclosing Risk policy.

3 Is there any risk in disclosing information to a representative or advocate?

4 If an individual consents to disclosure of information about risk to them, how far down the formal risk disclosure process (in terms of approval etc.) do we need to go?

5 Are we not limited in what we can actually do about risks to others?

6 Will there be any further training for staff?

7 Is it appropriate to tell someone on the phone that I have concerns about what they are saying and that I may need to speak to a manager and make a disclosure about this?

Answers

1 **Do we have a named person within PHSO responsible for child protection who we can discuss any child protection concerns we may have when disclosing information about risk?** 0 comments Back to Top

> No we do not currently have a dedicated staff member who deals with child protection concerns. If you have such a concern you should discuss it with your manager in the first instance.

2 **It would be helpful to have a list of all E2s and their contact details alongside the Disclosing Risk policy.** 0 comments Back to Top

> This link provides the details of all E2 and E1 Managers across PHSO and their contact telephone numbers. This will be regularly reviewed and updated.

3 **Is there any risk in disclosing information to a representative or advocate?** 0 comments Back to Top

> There should be minimal risk as we will already have the complainant's consent to disclose any information about the complaint to their representative or advocate. We should still bear in mind that in making a disclosure we should disclose the minimum amount of information to the minimum number of people/organisations.

4 **If an individual consents to disclosure of information about risk to them, how far down the formal risk disclosure process (in terms of approval etc.) do we need to go?** 0 comments Back to Top

> It is important to ensure that we consistently follow the procedure for disclosing risk as set out in paragraphs 13 and 14 even if the individual consents to the disclosure.

5 **Are we not limited in what we can actually do about risks to others?** 0 comments Back to Top

> In some cases there may be no one appropriate we can disclose to or little that we can do to assist. The policy says that we should disclose the minimum amount of factual information needed to mitigate the risk to the minimum number of organisations. In cases where we consider that there is no one we can reasonably disclose information to, it would not be appropriate to go ahead and disclose to anyone and everyone just in case.

6 **Will there be any further training for staff?** 0 comments Back to Top

> Learning and Development are currently in discussions with providers about further training for staff. This training is likely to focus on Dealing with Difficult Contacts and Dealing with threats of Suicide and/or Self-harm. The dates and format of the sessions has not yet been decided.

7 **Is it appropriate to tell someone on the phone that I have concerns about what they are saying and that I may need to speak to a manager and make a disclosure about this?** 0 comments Back to Top

> Yes if you feel comfortable taking this approach. The policy is flexible and offers a framework for managing behaviour. Whilst it details certain considerations that should be made, how each individual case is dealt with is subjective and will depend on the individual circumstances of the situation.

Unreasonable behaviour policy

Policy statement[1]

1. The Ombudsman is often the last resort for people who feel that their complaint has not been addressed and we want to make sure that we have fully understood the issues that they raise with us.

2. We are committed to dealing with all people fairly and impartially and to providing a high-quality service. As part of this service we do not normally limit the contact that people have with this Office. However, we do not expect our staff to tolerate behaviour that is, for example abusive, offensive or threatening, or which because of the frequency of the contact, makes it difficult for us to consider complaints. We will take action to manage such behaviour. As well as covering direct contact with the office, this policy may also take into account behaviour in other forums, such as on social media.

3. We will make every effort to make sure that our service is accessible to everyone. To achieve this outcome we will make reasonable adjustments to meet the individual and particular needs of anyone who contacts us. We are also committed to protecting the safety and welfare of our staff, and while we make every effort to provide an accessible service, the safety of our staff and giving them an environment free from fear and intimidation is very important to us.

1 Paragraphs 1-8 are the policy statement that should be sent to a person when a warning is applied. This text should also be used for the policy statement on the website.

4. When we consider that a person's behaviour is unreasonable we will tell them why we find their behaviour unreasonable and we will ask them to change it. If the unreasonable behaviour continues, we will take action to restrict the person's contact with our Office.

5. The decision to restrict access to our Office will only normally be taken after we have considered possible adjustments to our service which may help the person to avoid unreasonable behaviour. The decision will normally be taken by an operations manager at assistant director level[2] or above (or by the head of the review team or the Ombudsman's casework manager). Any restrictions imposed will be appropriate and proportionate. The options we are most likely to consider are:

- asking for contact in a particular form (for example, letters only);
- only allowing contact with a named officer;
- restricting telephone calls to specified days and times;
- asking the person to enter into an agreement about their future conduct; and/or
- actions designed to specifically meet the needs of the person.

6. In all cases we will write to tell the person why we believe their behaviour is unreasonable, what action we are taking and how long that action will last. We will also tell them how they can challenge the decision if they disagree with it.

7. If, despite any adjustments we have made, a person continues to behave in a way which is unreasonable, we may decide to end contact with that person.

8. We take the safety and welfare of our staff very seriously and will not tolerate any behaviour that threatens this. Where the behaviour is so extreme that it threatens the immediate safety and welfare of the Ombudsman's staff or others, we will consider other options, for example, stopping all contact immediately, reporting the matter to the police or taking legal action. In such cases, we may not warn the person before we do this.

What is unreasonable behaviour?

9. It is difficult to define what constitutes unreasonable behaviour. That will depend very much on the individual situation of the person concerned. However, any behaviour that makes someone feel uneasy, uncomfortable, distressed, anxious or unsafe is likely to be unreasonable. The policy statement gives examples of behaviour that

2 This can be any operations manager at E2 level or above.

is abusive, offensive or threatening and also explains how the level of contact hinders our consideration of complaints.

10. Unreasonable behaviour can occur in a variety of circumstances including in person, on the telephone, in written or email correspondence or on social media. We should take into account the type, frequency and content of contact as well as the level of disruption caused and the impact of the behaviour on the member of staff. It is not a requirement for everything mentioned in the policy statement to be present for the policy to be used. For example, a series of disruptive calls which contain no abusive content may be suitable for action to be taken under this policy as might a single call which contains a specific threat against a member of staff. If you consider that the person's behaviour may pose an immediate threat to the health, welfare or safety of our staff please refer to the information in paragraph 41 and at Annex C.

11. When making judgments about what is unreasonable behaviour we will take into account any relevant equality or diversity issues. For example, a complainant with a disability might find it difficult to behave in a way that we consider reasonable unless we have considered, and have made adjustments to our service, where appropriate, to make this possible.

Social media

12. If a person displays unreasonable behaviour on social media (for example, Facebook or Twitter) then we can consider using this policy to try to manage it. However, it is important that contact with a person in those circumstances is taken offline. This is in order to prevent personal or confidential information (either about a complaint or about a member of staff) being disclosed or publicised further. For example, if a person makes an offensive post then do not respond to it or issue a warning using the social media site. Instead, contact the person directly using telephone, letter or email.

13. If you see a social media post about a specific member of staff, this should be referred to the relevant staff member and/or their line manager. The line manager should then take responsibility for agreeing what action to take. The following options can be considered:

    - support for the employee (including employee assistance programme);
    - notifying the employee relations manager and web editor;
    - asking the person who made the post, or the social media platform, to remove it
    - reporting the person to the social media platform (if the behaviour persists)

- seeking advice from the legal team.

Process

14. The key elements of the process (which are also summarised in the process flowchart (see page 11) are listed below. (Note: It is only necessary to move to the next step of the process if the person's behaviour continues to be unreasonable.)

- Tell the person that we consider their behaviour to be unreasonable and why.
- Consider if a new or existing advocate can be used to communicate with the person.
- Issue a warning and policy details in writing with the agreement of a manager.
- Escalate to an operations E2 level manager or above (or to the head of review team or Ombudsman's casework manager) to consider applying the policy. They will take a decision on:
    - requirements/conditions for the person to follow in order to manage their behaviour.
    - Advice and support to staff who receive contact from that person.
    - Date for review of requirements/conditions.
    - Responsibility for handling requests for review of requirements /conditions.

Tell the person that we consider their behaviour to be unreasonable and why

15. If a complainant behaves unreasonably then it is important that we tell them that we consider their behaviour unreasonable, explain why, give them the opportunity to stop and consider whether we can adjust our service to help them do this. (Note: this explanation can, if necessary, be given at the same time as a warning about the potential application of this policy).

16. If a member of staff does not feel comfortable in challenging unreasonable behaviour, or is concerned that their personal safety is at risk if they were to do so (particularly if the behaviour is threatening and/or occurs in a face-to-face setting such as a visit or interview) it is important that the details of the complainant's behaviour are noted on Visualfiles as soon as possible after the event and discussed with line managers to allow appropriate action to be taken.

17. Examples of when and how to challenge unreasonable behaviour:

- If a complainant uses offensive language during a telephone call then staff should explain to them that their use of such language is unreasonable and ask them to stop. For example, by simply saying 'Please don't swear at me'. If the complainant refuses to comply with that request then staff should advise them politely that the call will be terminated and then end the call. The staff member should add a note of the call and the reasons for terminating it to Visualfiles as soon as possible and discuss the call with a manager.

- If a complainant uses offensive language in letters or emails, our next written response to them should explain that the language they have used is unreasonable and ask them not to do this in future correspondence.

- If a complainant makes repeated telephone calls without legitimate purpose (for example, to ask about progress on their case when they have recently been given that information) staff should explain to them that their behaviour is disruptive to the staff being contacted and is preventing work on their case and others; they should ask the complainant to stop doing this. If the complainant refuses to comply with that request then further calls can be terminated politely after a brief explanation (for example, that we have nothing further to add to the last update given on the case).

- If a complainant sends repeated letters or emails without legitimate purpose (for example, if they send one letter each day that does not add anything to the evidence in support of their case), our next written response to them should ask them to limit the amount of correspondence.

18. It is important that we log full details of any behaviour we consider to be unreasonable by complainants on Visualfiles. This should include the type and frequency of contacts and details of, for example, offensive terms used. So, instead of saying 'During the call Mr A made a number of racist remarks', we should record explicitly the language used and give as much information as possible about how and when it was used. This should not only include what someone said or did but their manner when they spoke or acted in that way.

19. In all cases of unreasonable behaviour the member of staff should seek support from their line manager. If we are aware of specific reasons for such behaviour, we should consider an appropriate plan to manage it.

Consider if a new or existing advocate can be used to communicate with the person

20. When we seek to manage a complainant who is displaying unreasonable behaviour we should consider approaching their advocate or representative (if they have one) at an early stage to ask

for their assistance in understanding and managing the behaviour. We could also suggest that they consider getting an advocate (for example, POhWER, SEAP or NHS Complaints Advocacy). This may be particularly relevant if there are equality or diversity issues (for example, if the complainant has a disability that which directly affects their behaviour).

Issue a warning and policy details in writing with the agreement of a manager

21. A warning will normally be given to the person before we apply the policy. The member of staff dealing with the case can do this, or another member of staff as appropriate. The warning should explain what the behaviour was, why we consider it to be unreasonable and the likely consequences of any continuation.

22. The person concerned should also be sent a copy of the policy statement (paragraphs 1-8 above; also available on PHSO's website). Ideally, warnings will be given in writing because this gives the person a clear statement and leaves an audit trail. If it is necessary to give a warning over the telephone or face to face, a copy of the policy statement should be sent to the person as soon as possible afterwards, with a brief letter reiterating the warning. A letter of warning should (if appropriate) also make clear our willingness to discuss a reasonable adjustment to our service if this would be helpful.

23. If a Member of Parliament and/or a representative has been involved in the case, we should also tell the person that, if the unreasonable behaviour continues and we decide to apply our policy, we will tell the MP and/or the representative.

24. The decision to issue a written warning should be discussed in advance with a manager. If a member of staff gives the warning in a telephone call or face to face setting, they should inform a Manager as soon as possible after the event.

25. A warning should be recorded fully on the individual's details screen on Visualfiles (this screen can be accessed by either searching for the individual by name or by accessing their person details from a case).

    - On the individual's screen select '*Behaviour policies'* then '*Apply warning' (*if a previous warning exists, the option to '*View existing warnings*' or '*Create a new warning*' appears).
    - Complete the mandatory comments box. This should summarise the reasons for giving the warning and contain a brief note of the discussion with the manager.
    - Select the manager with whom the warning was discussed from the list of staff.

26. Existing (or previous) warnings are available by selecting '*View warnings'* from the *'Behaviour policies'* screen.

27. If the person's behaviour is particularly serious (for example, a specific and immediate threat to a member of staff), a decision may be taken at operations E2 manager level or above (or by the head of the review team or the Ombudsman's casework manager) to apply the policy without prior warning to the complainant. In that event, the member of staff who authorises the application of the policy will write immediately to the person explaining the reasons for doing so.

Escalate to consider application of the policy

28. If the person continues to behave in a way that is unreasonable, then a request to apply the policy should be referred to an Operations manager at E2 level or above (or to the Head of the Review Team or the Ombudsman's casework manager). This request should provide relevant details (for example, steps taken so far, nature and frequency of the behaviour, information about the complainant's needs and circumstances (if known), and the type and duration of any proposed requirements or conditions).

29. The decision on whether to apply the policy will be recorded on Visualfiles. This should include whether restrictions need to apply to any other existing enquiries, reviews, investigations or information requests that the person has with PHSO.

30. If the Office decides not to apply the policy then the manager who considers the request will decide how to manage contact from the person in the future.

31. If the policy is applied, we will balance the interests of the person with the duty to protect the health, safety and welfare of our staff. Possible actions include:

    - requesting contact in a particular form (for example, letters only);
    - requiring contact to take place with a named officer;
    - restricting telephone calls to specified days and times;
    - asking the person to enter into an agreement about their conduct; and/or
    - actions designed specifically to meet the needs of the person.

32. We should consider whether we should inform the Security Officer. This is particularly relevant when staff have felt threatened by the actions of a person.

33. The action will be applied for a set period and we will set a review date not more than 6 months after any conditions are imposed.

34. The manager applying the restrictions will then send a letter to the person including the following:

    - the reasons for the decision;
    - the requirements/conditions the person must follow and any adjustments we will make to assist this;
    - the date set for review;
    - how the person can challenge the decision;
    - a warning that continued unreasonable behaviour may lead to the case being closed; and
    - where relevant, that the MP/representative has been told of the action.

35. A decision to apply the policy should be recorded fully on Visualfiles by (or on behalf of) the person approving the decision.

    - On the individual's screen select 'Behaviour policies' then 'Apply policy'.
    - Select the manager who approved the decision to apply the policy.
    - Select the date on which the application of the policy should be reviewed.

36. Add relevant details about the restrictions imposed.

    - Select 'Add/view restrictions' (if previous restrictions exist the option to 'View existing restrictions' or 'Create a new restriction' appears).
    - Choose the restriction type from the list that appears.
    - Complete the mandatory comments box. This should summarise the restrictions imposed.
    - Select the manager with whom the application of the restriction was discussed (note: in many cases this will be the manager who authorised the application of the policy).

37. Existing or previous restrictions can be viewed by selecting 'Add/view restrictions' and then '*View existing restrictions*'.

38. In the face of continued unreasonable behaviour an operations director (or above) may decide to terminate contact with a complainant completely (which would also have the effect of closing/discontinuing any active assessment, investigation or review under consideration by PHSO at that time). This may be appropriate, for example, where a person refuses to comply with restrictions on contact that we have imposed under this policy. In such cases we will read all correspondence from that complainant, but will send an acknowledgement only unless there is fresh evidence which affects our decision on the complaint.

39. It is essential that the information relating to the application of this policy on Visualfiles is kept updated, particularly if the restrictions on contact are altered/varied or removed.

Complaints about decisions to apply the policy

40. If a person disagrees with the decision to apply the policy, they can ask the line manager of the person who agreed the restrictions to review the application of the policy. The member of staff carrying out that review must issue a written decision to explain the outcome.

Extreme behaviour

41. In exceptional cases, the behaviour of the person may pose an immediate threat to the health, welfare or safety of our staff. In such circumstances, an operations manager at E2 level or above (or the head of the review team or the Ombudsman's casework manager) may decide to take action without prior warning to the person such as terminating all contact. They may also consider other action such as police involvement. A record must be kept of this decision, clearly recorded on Visualfiles and notified to the line manager of the member of staff who approved this action and to the security officer. A risk assessment template and guidance on completing a risk assessment are available (see Annex C for details).

Modification of behaviour

42. If at any point before the review date the person modifies their behaviour to the extent that the restrictions should no longer apply, then a proposal to remove the restrictions can be agreed at operations E2 manager level or above (or by the head of the review team or the Ombudsman's casework manager). If restrictions are removed before the set review date then the person should be told in writing. This should also make clear that if the previous behaviour resumes this could lead to restrictions being reimposed or further restrictions imposed.

Deciding whether to keep applying the policy at the review date

43. The manager who agreed the restrictions will normally carry out the review. The reviewer will take into account the evidence and reasons

for making the original decision, and any evidence of the person's subsequent behaviour. The reviewer will also seek comments from appropriate staff, including those affected by the behaviour, and consider the effectiveness of any adjustment we have made.

44. If the reviewer decides not to extend the original restrictions for a further period, the conditions imposed on the person will lapse. If, at the time of the review, there is continuing contact with the person, the reviewer will write to the person explaining the decision. The decision will also be noted on Visualfiles. If the person is not in regular contact then we will not re-establish contact to tell them about the decision, but will advise them of the decision if and when they make contact again. If the reviewer does not extend the original decision and the unreasonable behaviour occurs again at a later point we may choose to return to the previous restrictions without going through the warning stages.

45. If the reviewer decides to extend the original decision, they will set a further period of a maximum of twelve months. When this expires, there will be a further review.

46. The review of the policy should be recorded fully on Visualfiles by (or on behalf of) the person carrying out the review.

- On the individual's screen select 'Behaviour policies' then 'Policy review'.
- Select the manager who reviewed the application of the policy.
- Select the outcome of the policy review: 'Continue', 'Revised restrictions' or 'End application of policy'.
- If 'Continue' or 'Revised restrictions' are selected then a further review date must be entered.
- Before 'End application of policy' can be recorded there must be no current restrictions in place. To end a current restriction select 'Add/view restrictions' and then 'View existing restrictions'. Highlight the relevant restriction and then press 'Select restriction'. You can then select 'End date' and will be prompted to enter the name of the manager who approved the ending of the restriction (which may also be the manager who reviewed the application of the policy).

Further complaints and information requests

47. Restrictions under this policy are generally applied to an individual. However, there may be circumstances in which we apply restrictions on a case-specific basis. This will depend on the individual circumstances of the case.

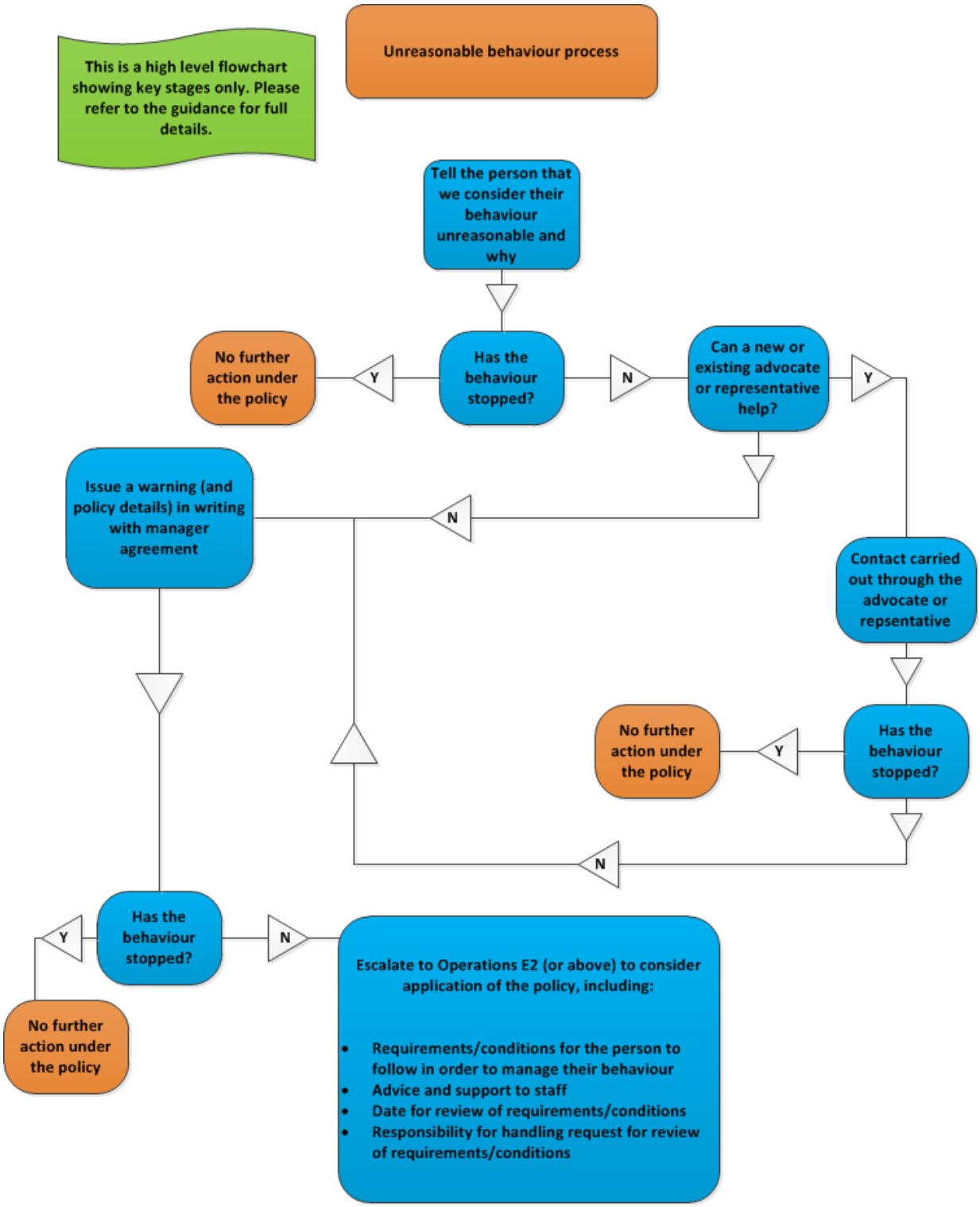
48. If a person who has had restrictions applied under this policy seeks to make a fresh complaint, consult an operations manager at E2 level or above (or the head of the review team or Ombudsman's casework manager) (normally the manager who applied the policy) in order for a decision to be reached on how to respond to that further contact.

49. If a person who has had restrictions applied under this policy makes a Freedom of Information request or Data Protection Act subject access request then an operations manager at E2 level or above (or the head of the review team or Ombudsman's casework manager) (normally the manager who applied the policy) and head of FOI/DPA should be consulted for advice.

Variation of these procedures

50. These procedures may be varied in individual circumstances or on a specific issue by agreement with a member of staff at director level or above.

Annex A Unreasonable behaviour process flow chart



Annex B example letters

Warning letter

I write in response to your telephone calls to me and my colleague yesterday. During these telephone calls, you made numerous abusive comments to us which we found offensive. When speaking to staff at our Office it is unacceptable to swear or make racist comments or comments of a sexual nature.

Please stop making such comments or being at all rude to staff. If you continue to contact us in this way, we may unfortunately have to take steps to manage our communication with you which may include limiting your contact with us. I enclose the Ombudsman's Unreasonable Behaviour Policy, which you can find on our website at…

That said, if you are prepared to have a polite and reasonable conversation about your complaints, we will be happy to discuss them with you.

Letter imposing restrictions

As you know, we warned you that if you continued to swear or use racist and/or sexual language when talking to our staff then we would consider taking action to limit your contact with us. Despite that letter and further reminders you have continued to use inappropriate and offensive language when talking to staff. As your offensive remarks have fallen within our definition of 'unreasonable behaviour' I have instructed my staff not to take telephone calls from you.

Consequently, you are now prohibited from making telephone calls to us but you may still communicate in writing. To be clear, you must not use the telephone to contact this office. If you do so, my staff will immediately terminate the call. However, we will review the position in six months.

If you have any representations then please send them to us in writing and we will consider your concerns.

I hope you understand that this action has become necessary because of the abusive nature of your telephone calls. We will continue to deal with written communication, that is not of an abusive nature, in an appropriate manner.

Annex C: Employee risk assessment process

1. Security at PHSO is the collective responsibility of all staff and contractors. It is supported by a clear corporate accountability framework, designating specific roles and responsibilities as set out in the Security Policy.

2. The employee risk assessment form is intended to be used when a potential risk to the safety or wellbeing of a PHSO member of staff is identified from a complainant or another party to the complaint.

3. Any employee identifying a potential risk to themselves or another member of staff should talk immediately to their line manager (or another manager if the line manager is not available). The line manager (talking to others as necessary) should then decide whether the employee risk assessment form should be completed (as there may be circumstances in which no action or different action is required).

4. Examples of circumstances in which this form could be used:

    - Threats to members of staff (for example, in letters, emails, telephone calls or face-to-face).
    - Nuisance telephone calls or emails.
    - Members of staff being contacted or approached by a complainant outside of work.

5. These are only examples. The key factor in deciding whether to use the form should be the identification of the risk to the member of staff. A flowchart is available that summarises the process for using this form.

Completing the form

6. The line manager of the member of staff at risk should complete the form.

7. The form is a living document and should be reviewed and revised when necessary. Additional sheets are available to record further actions and review dates.

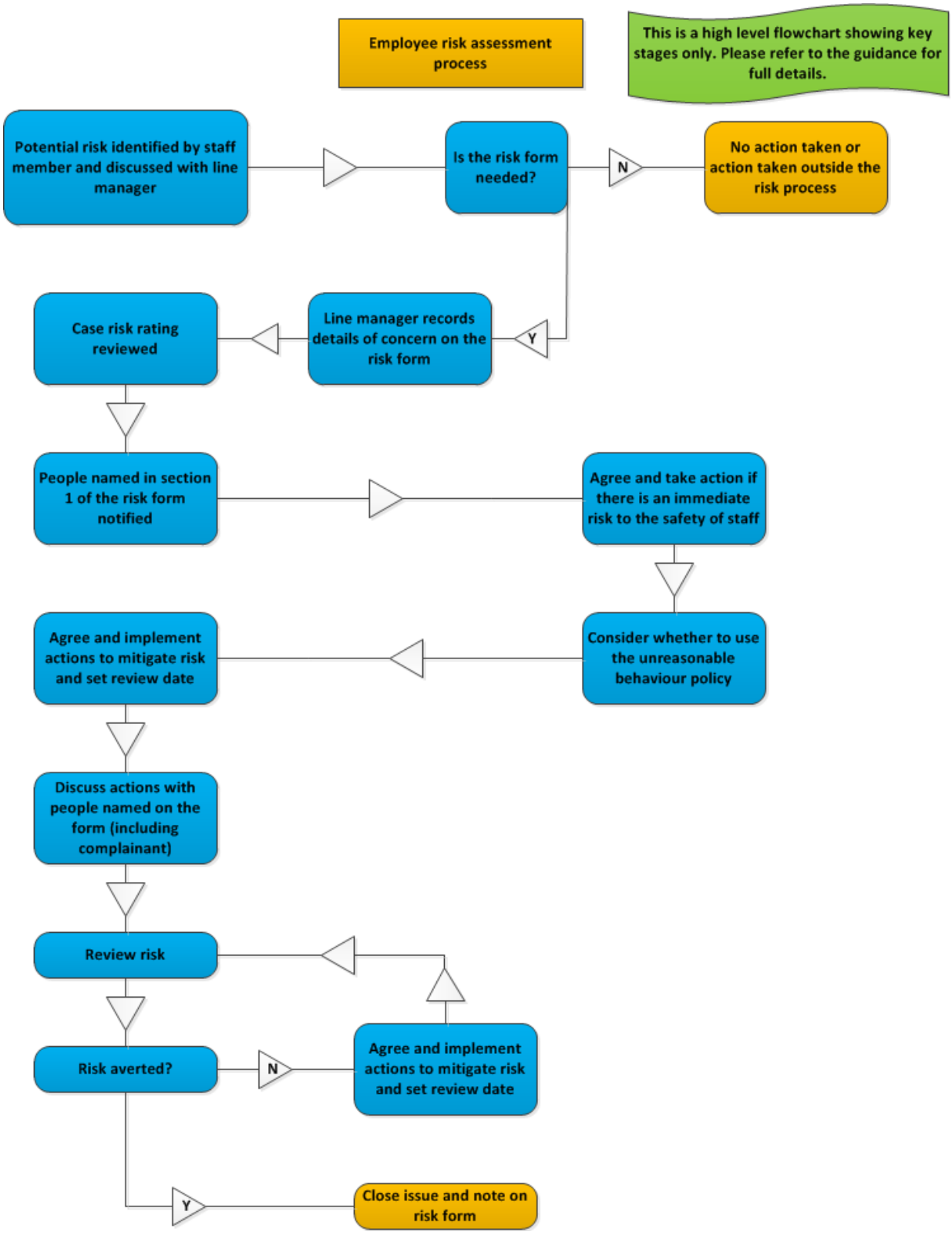
8. The form should be saved on the relevant Visualfiles case record.

9. If you need further advice please talk to your line manager in the first instance.

    - Section 1: Complete the names of relevant staff, case reference number and date. The ‘staff support’ field is optional and is intended to record details of anyone who is supporting the staff member such as a trade union representative or other colleague.
    - Section 2: A summary of the risk, how it was identified, relevant dates and any action taken so far. This must also say whether the relevant case is open or closed.

- Section 3: This should be ticked when the case risk rating has been reviewed.
- Section 4: This should be ticked when the security officer has been notified.
- Section 5: Answer yes or no to the three questions about immediate risk and reallocation of the case.
- Section 6: This should be ticked once application of the unreasonable behaviour policy has been considered.
- Section 7: A summary of the agreed actions, who will carry them out and by when. This will include internal actions (for example, issuing a warning or imposing a restriction under the unreasonable behaviour policy) and external actions (for example, contacting the police).
- Section 8: A date to review the risk again should be agreed and entered here. The timescale for this will depend on the circumstance of the case, but it should not be more than three months from the completion of the form. The risk can of course be reviewed prior to that date if circumstances change.
- Section 9: The line manager should tell relevant people (both internally and externally) about the agreed actions (section 7) and tick to confirm it has been done. This will include telling those people named in section 1 of the form. It may also involve contacting the complainant or other parties to the complaint.
- Section 10: This should be used to record the outcome of the risk review (which should happen at the latest by the date set in section 8).
- Section 11: Record if the risk can now be closed. If not, the risk should be reviewed and further action agreed (as per section 7).
- Section 12: The form should be signed by the relevant members of staff after section 8 has been completed.

- **Employee risk assessment flowchart**



Quality & Service Integrity > FAQs

Menu

FAQs

Category Unreasonable behaviour

Questions

1. Is there anything on our external website with our policy statement or what we can expect from customers like a customer charter?
2. Can we have a steer about what information staff can put on their own social media accounts in relation to personal and job info?
3. Is there any way of protecting ourselves from an adverse impact of an increased social media presence now that we have opened ourselves up to the wider public via Facebook, Twitter etc.
4. How much input would the caseworker have into what action would be taken to mitigate a risk to staff or unreasonable behaviour?
5. Do we know how many times we have issued a warning under the Unreasonable Behaviour policy and how many times we have had to apply the policy?
6. Will we be reviewing historical cases with warnings on them in case complainants come back to us at some point?
7. Will the new CMS be able to bring up warnings previously issued on other cases? Is there/will there be a formal way of recording an application of the policy or issuing of a policy warning so that this information is all contained in one place on VF/CMS.
8. Do we need to tell complainants that we have reviewed the restrictions in place under the Unreasonable Behaviour policy if they have not been in touch with us for some time?
9. If we have terminated all contact and closed all open cases under the Unreasonable Behaviour policy, do we still have to look at any new complaints that the complainant may bring to us?
10. Could we seek input from other areas of the office when considering putting restrictions in place - for example if we want to restrict after the case has closed we might ask the review team for input.
11. Is there any problem applying the Unreasonable Behaviour policy or reviewing a restriction even if the case is closed?
12. Should we involve the legal team in cases of persistent unreasonable behaviour?
13. Can we block numbers of persistent callers?
14. If a complainant asks to only have their case dealt with by a member of staff of a particular gender or from a particular ethnic group, would that be dealt with under the policy and how?
15. Do we disclose the location/address of the Exchange if asked?
16. I have concerns that our approach towards unreasonable behaviour is not consistent across the office, including senior staff.
17. Can we be challenged on decisions to apply the policy and restrict contact?
18. Can we issue a warning at the same time as telling someone their behaviour is not acceptable?
19. What do we do in situations where a case has been closed, and the complainant continues to contact us. There is nothing further we can do to assist them and they are not disruptive, abusive or threatening, just irritating.
20. If someone is venting and ranting on the phone but I am comfortable continuing to communicate with them despite this behaviour, would it be appropriate to make a note on VF of my decision to not to impose the policy or a warning?
21. Do we have a zero tolerance policy?

Answers

1 Is there anything on our external website with our policy statement or what we can expect from customers like a customer charter? 0 comments Back to Top

> The **Unreasonable Behaviour policy statement** (the first eight paragraphs of the Unreasonable Behaviour policy) is on PHSO's external website under Complaining about our Service. This explains that we will not tolerate any behaviour that threatens the welfare and safety of our staff and details the actions we will take in circumstances where such behaviour occurs.

2 Can we have a steer about what information staff can put on their own social media accounts in relation to personal and job info? 0 comments Back to Top

> The ICT Acceptable Use Policy paragraph 12 provides some guidelines for staff on what not to put on their own personal social media accounts.

3 Is there any way of protecting ourselves from an adverse impact of an increased social media presence now that we have opened ourselves up to the wider public via Facebook, Twitter etc. 0 comments Back to Top

We cannot control what individuals say about us on social media sites. If someone is displaying unreasonable behaviour through social media then we can manage that behaviour by using the policy. Paragraphs 12 and 13 of the policy provide further detail about social media. Essentially, the matter should be escalated to a manager and any action taken should be carried out off line.

4 **How much input would the caseworker have into what action would be taken to mitigate a risk to staff or unreasonable behaviour?** 0 comments Back to Top

There should always be a discussion between the caseworker and their manager to discuss the most appropriate steps to mitigate risk or manage unreasonable behaviour. How much input the caseworker provides will depend on them, their manager and the situation. We should ensure that our actions are the most appropriate ones for managing the situation.

5 **Do we know how many times we have issued a warning under the Unreasonable Behaviour policy and how many times we have had to apply the policy?** 0 comments Back to Top

Over the past three years we have issued a warning approximately 80 times, although in some cases the same individual has had more than one warning. We have restricted contact under the policy 19 times; again some individuals have had more than one restriction applied to them.

6 **Will we be reviewing historical cases with warnings on them in case complainants come back to us at some point?** 0 comments Back to Top

We are currently looking at reviewing restrictions applied on historical cases.

7 **Will the new CMS be able to bring up warnings previously issued on other cases? Is there/will there be a formal way of recording an application of the policy or issuing of a policy warning so that this information is all contained in one place on VF/CMS.** 0 comments Back to Top

How we record information about issuing warnings and applying the policy has been raised with those leading on designing the new CMS and discussed for inclusion in the high level blueprint. The next stage will look at this in more detail.

8 **Do we need to tell complainants that we have reviewed the restrictions in place under the Unreasonable Behaviour policy if they have not been in touch with us for some time?** 0 comments Back to Top

No. Paragraph 44 of the policy says that if the person to whom we applied the policy to is not in regular contact with us then we will not re-establish contact to tell them about the decision. We will advise them of the decision if and when they make contact with us again.

9 **If we have terminated all contact and closed all open cases under the Unreasonable Behaviour policy, do we still have to look at any new complaints that the complainant may bring to us?** 0 comments Back to Top

Yes. We cannot refuse to accept new complaints even if our previous relationship with the complainant has meant terminating all contact and closing open cases. However, when looking at a fresh complaint we should talk to the staff previously involved with the case and have a management plan in place should the behaviour recommence.

10 **Could we seek input from other areas of the office when considering putting restrictions in place - for example if we want to restrict after the case has closed we might ask the review team for input.** 0 comments Back to Top

Yes. The types of restrictions considered will be dependent on the type of behaviour being exhibited. Seeking input from other parts of the office in order to determine what restrictions are most appropriate can be a useful tool.

11 **Is there any problem applying the Unreasonable Behaviour policy or reviewing a restriction even if the case is closed?** 0 comments Back to Top

No. The policy is a framework to assist us in managing an individual's behaviour, regardless of what stage the case is at. Even if the case is closed it may be being dealt with by another part of the office and therefore we will still need to manage the behaviour.

12 **Should we involve the legal team in cases of persistent unreasonable behaviour?** 0 comments Back to Top

The legal team have advised that it may worthwhile contacting them specifically on cases where staff are being harassed and/or defamed. If you think it may be appropriate to contact the legal team about a case, speak to your manager first.

13 **Can we block numbers of persistent callers?** 0 comments Back to Top

We do not block the numbers of persistent callers. We manage their behaviour using the Unreasonable Behaviour policy.

If a complainant asks to only have their case dealt with by a member of staff of a particular gender or from a

14 **particular ethnic group, would that be dealt with under the policy and how?** 0 comments Back to Top

> Unless they are behaving in an unreasonable way in making that request, it is unlikely that situation would be covered by this policy. This example appears to relate more to Equality and Diversity issues which should be flagged with a manager in the first instance. All requests should be dealt with on a case by case basis as we will want to understand the reasons for such a request.

15 **Do we disclose the location/address of the Exchange if asked?** 0 comments Back to Top

> Yes unless we consider there to be an imminent risk/danger to staff if we disclose the information.

16 **I have concerns that our approach towards unreasonable behaviour is not consistent across the office, including senior staff.** 0 comments Back to Top

> We should try to ensure consistency across the office when it comes to applying the policy but there may be reasons when it is appropriate to take a different approach. The policy is designed to be a framework for decisions: it does not prescribe when actions should be taken. We want to encourage people to challenge unreasonable behaviour and, where appropriate, issue warnings, in order to provide a firm foundation for action that might be needed later on. We also want to make people contacting us aware that we might take action if they continue to behave in a certain way.

17 **Can we be challenged on decisions to apply the policy and restrict contact?** 0 comments Back to Top

> Yes the individual against whom we have applied the policy can complain about that decision. Paragraph 40 of the policy explains that if a person disagrees with the decision to apply the policy, they can ask the line manager of the person who agreed the decision to issue a warning or apply the policy to review that decision. The member of staff carrying out that review must issue a written decision to explain the outcome.

18 **Can we issue a warning at the same time as telling someone their behaviour is not acceptable?** 0 comments Back to Top

> Yes. The policy allows (see paragraph 15) for a flexible approach so if it is appropriate to do so, we can issue the warning and use this as the first opportunity to tell the person that their behaviour is unacceptable and why.

19 **What do we do in situations where a case has been closed, and the complainant continues to contact us. There is nothing further we can do to assist them and they are not disruptive, abusive or threatening, just irritating.** 0 comments Back to Top

> In the past, we have applied a 'Do Not Acknowledge' instruction to closed cases where the complainant has persisted in sending regular, repetitive correspondence that has contained nothing new of substance in relation to their complaint. We are looking at whether it would be appropriate to return to this approach. Once we have determined the best way to proceed in these situations we will update staff.

20 **If someone is venting and ranting on the phone but I am comfortable continuing to communicate with them despite this behaviour, would it be appropriate to make a note on VF of my decision to not to impose the policy or a warning?** 1 comment Back to Top

> Staff will have different views about what they are willing to tolerate. If you feel comfortable continuing to communicate with the complainant despite their behaviour then a warning does not have to be issued, though the reasons for not doing so should be recorded on VF. However, we should bear in mind that other colleagues may not be tolerant of this behaviour and the complainant may not be getting a consistent message if later down the line they are given a warning for exhibiting the same behaviour toward someone else. We should ensure we continue to monitor the behaviour and take appropriate action if necessary.

21 **Do we have a zero tolerance policy?** 0 comments Back to Top

> No. The aim of the Unreasonable Behaviour policy is to assist us in managing an individual's behaviour to allow us to carry out our role of investigating complaints. Our aim is to still be able to deal with their complaint and bring it to the most appropriate conclusion. We do not want to apply the policy at the first sign of unreasonable behaviour.

Menu

FAQs

Category Risk to staff

Questions

1. **Is the risk to staff form for managers to complete available on VF or Ombudsnet?**
2. **Where there is a risk to staff what sort of action might we take to prevent the risk?**
3. **Does the risk to staff guidance overlap with risk assessment for staff going out to conduct interviews?**
4. **Do we still have guidance on threats to the Office (e.g. what to do if there is a bomb threat)?**
5. **If we have to take action to mitigate risk to a staff member do we tell the complainant why we have taken this action?**

Answers

1 **Is the risk to staff form for managers to complete available on VF or Ombudsnet?** 0 comments Back to Top

> This is a link to the **employee risk assessment form** which is contained within the **Disclosing Information about Risk policy** located on Ombudsnet on the Casework Policy and Guidance page. The form is not currently on VF, though we are discussing making it available on the new CMS.

2 **Where there is a risk to staff what sort of action might we take to prevent the risk?** 0 comments Back to Top

> This will depend on the type of risk. We may decide to issue a warning or apply the Unreasonable Behaviour and restrict the individual's contact with the office. We may decide to alert the PHSO Security Officer or in more serious cases, the police. We may decide to move the case to another colleague, or a different team or site. Most importantly, we should ensure that any actions we take are appropriate to the type of risk identified.

3 **Does the risk to staff guidance overlap with risk assessment for staff going out to conduct interviews?** 0 comments Back to Top

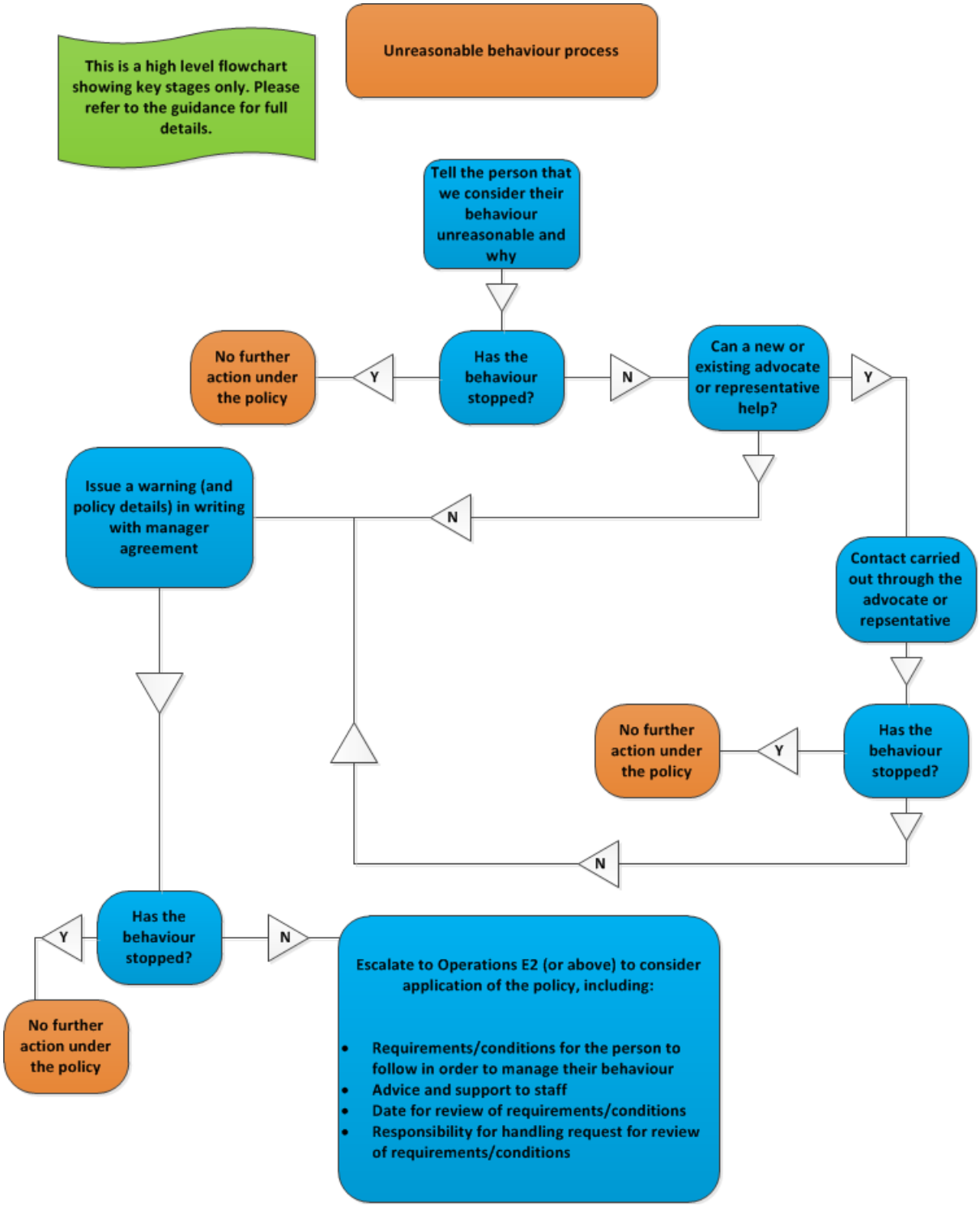
> The employee risk assessment form is intended to be used when a potential risk to the safety or wellbeing of a PHSO member of staff is identified from a complainant or another party. The form is focused on what actions we can take to mitigate that risk. It is unlikely to be appropriate to assess the risk for staff going out to investigate. We have raised the issue of carrying out off-site risk assessments with Facilities and will to work on some guidance to cover that in the new year. In the interim, if staff are going off-site for interview then they should discuss their personal security and any relevant risk elements with their line manager as part of the planning for that interview.

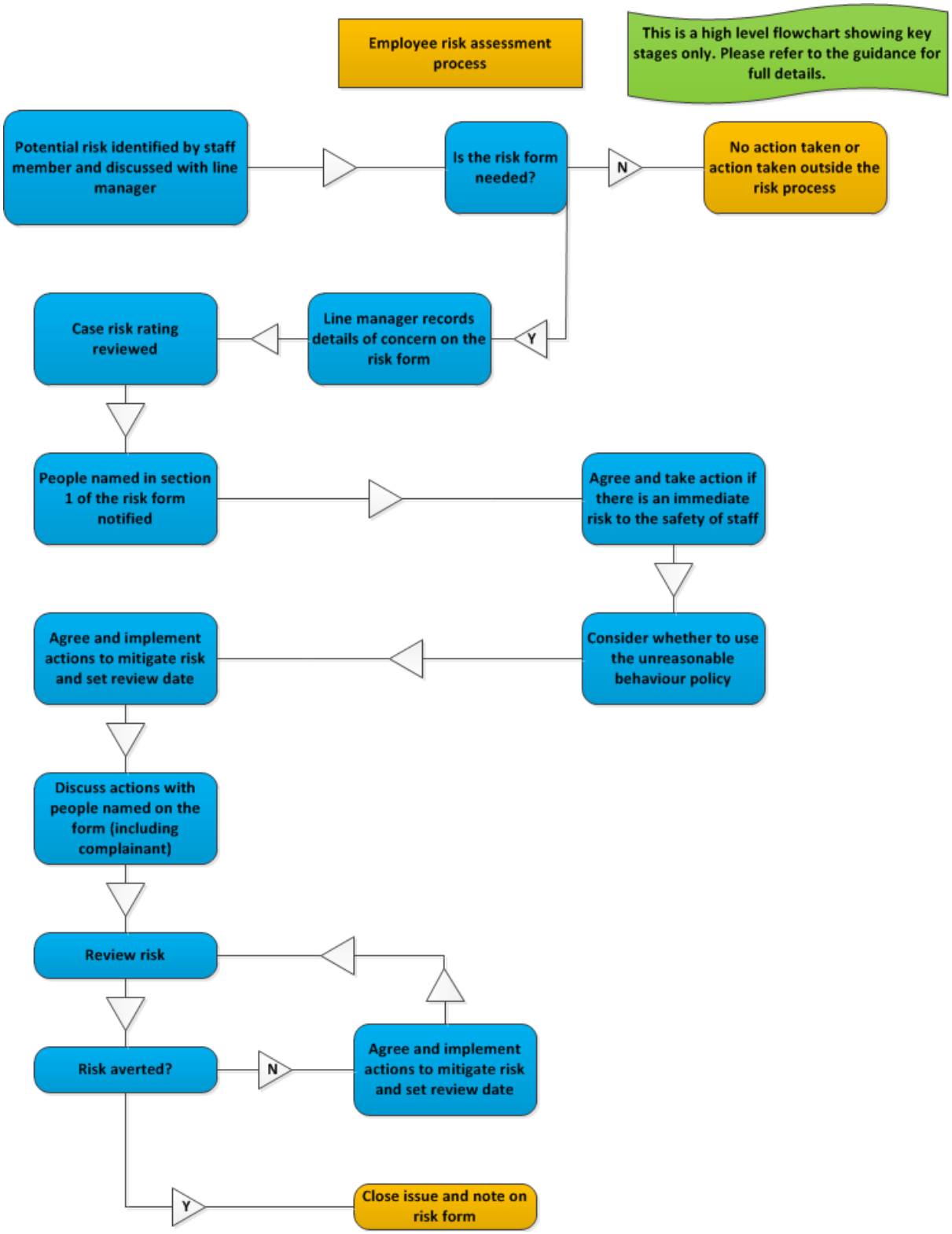
4 **Do we still have guidance on threats to the Office (e.g. what to do if there is a bomb threat)?** 0 comments Back to Top

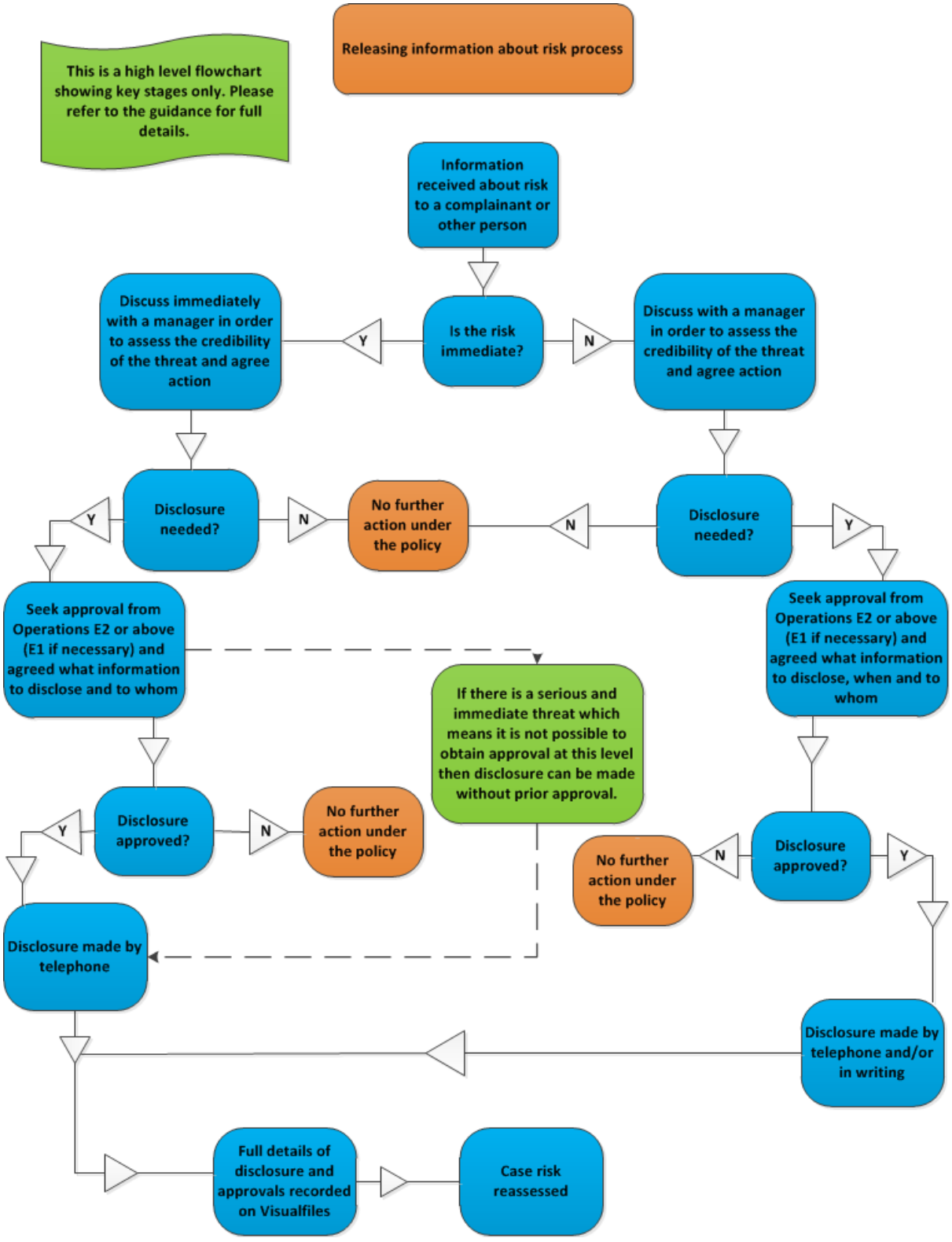
> Our **Health and Safety policy** contains details of fire procedures and other health and safety matters. Facilities are currently in the process of updating the Business Continuity Framework along with guidance on major incident evacuation procedures. Once these are approved they will be issued on Ombudsnet.

5 **If we have to take action to mitigate risk to a staff member do we tell the complainant why we have taken this action?** 0 comments Back to Top

> The policy does not say whether we should or should not tell the complainant. This would be dependent on a number of things including the nature of the risk and whether the staff member feels comfortable about telling the complainant the action we have taken and why. The policy allows for a flexible approach so if it is appropriate to do so, we can inform the complainant.


This is a high level flowchart showing key stages only. Please refer to the guidance for full details.
Unreasonable behaviour process
Tell the person that we consider their behaviour unreasonable and why
Has the behaviour stopped?
Y
No further action under the policy
N
Can a new or existing advocate or representative help?
Y
Contact carried out through the advocate or repsentative
N
Issue a warning (and policy details) in writing with manager agreement
Has the behaviour stopped?
Y
No further action under the policy
N
Has the behaviour stopped?
Y
No further action under the policy
N
Escalate to Operations E2 (or above) to consider application of the policy, including:
Requirements/conditions for the person to follow in order to manage their behaviour
Advice and support to staff
Date for review of requirements/conditions
Responsibility for handling request for review of requirements/conditions


Employee risk assessment process
This is a high level flowchart showing key stages only. Please refer to the guidance for full details.
Potential risk identified by staff member and discussed with line manager
Is the risk form needed?
N
No action taken or action taken outside the risk process
Y
Line manager records details of concern on the risk form
Case risk rating reviewed
People named in section 1 of the risk form notified
Agree and take action if there is an immediate risk to the safety of staff
Consider whether to use the unreasonable behaviour policy
Agree and implement actions to mitigate risk and set review date
Discuss actions with people named on the form (including complainant)
Review risk
Risk averted?
N
Agree and implement actions to mitigate risk and set review date
Y
Close issue and note on risk form


Releasing information about risk process
This is a high level flowchart showing key stages only. Please refer to the guidance for full details.
Information received about risk to a complainant or other person
Is the risk immediate?
Y
N
Discuss immediately with a manager in order to assess the credibility of the threat and agree action
Discuss with a manager in order to assess the credibility of the threat and agree action
Disclosure needed?
Y
N
No further action under the policy
N
Disclosure needed?
Y
Seek approval from Operations E2 or above (E1 if necessary) and agreed what information to disclose and to whom
Seek approval from Operations E2 or above (E1 if necessary) and agreed what information to disclose, when and to whom
If there is a serious and immediate threat which means it is not possible to obtain approval at this level then disclosure can be made without prior approval.
Disclosure approved?
Y
N
No further action under the policy
No further action under the policy
N
Disclosure approved?
Y
Disclosure made by telephone
Disclosure made by telephone and/or in writing
Full details of disclosure and approvals recorded on Visualfiles
Case risk reassessed

General Guidance: Disclosure of concerns about the health and safety of patients – section 15 Health Service Commissioner's Act (HSC)

Legislation

1. If during our consideration of a health case[1] we discover any information which may indicate a threat to the health and safety of patients, we should consider whether disclosure of those concerns to, for example, a regulatory body or employer, etc. might be appropriate.

2. We have a statutory power to disclose such information to any persons to whom we think the information should be disclosed to in the interests of the health and safety of patients[2].

3. If information is disclosed for this reason, both the person supplying us with the information and the subject of the information must be told that we have disclosed it and who we have disclosed to[3].

4. Information can be disclosed at any point that we consider necessary, subject to other relevant considerations such as fairness and reasonableness. For example, we do not need to wait until the end of our consideration of a case.

5. The relevant text from the Health Service Commissioners Act 1993 is attached at Annex A.

Background

6. Where we have evidence of concerns about the actions of individuals, it is important that we consider sharing that information with other parties with an appropriate interest in the matter. (**Note:** We do not **refer** individuals to their regulatory body or employer; we share information with them.)

7. Circumstances in which we may disclose are most likely, though not always, to arise in respect of clinicians. The sharing of concerns can often be dealt with through discussions with the employing or supervising NHS organisation as part

[1] Note: this is not restricted to investigations only. The Act refers to information obtained 'in the course of' or 'for the purposes of' the investigation. So this can also include information obtained by Customer Services at the enquiry/assessment/resolution stage or at the review stage.
[2] 1993 Act, section 15 (1) (e)
[3] 1993 Act, section 15(1) (c).

of our normal casework process without the need for disclosure under section 15.

8. However, cases occasionally arise when we need to consider whether such information should also be reported to a regulatory or other external body or to other individuals. For example, the General Medical Council (GMC), the General Dental Council (GDC), the Nursing and Midwifery Council (NMC), or the police. (**Note:** When we make findings against an individual doctor we usually share an anonymised version of the final report with the doctor's responsible officer[4] regardless of any Section 15 concerns).

9. A disclosure under Section 15 is a significant step to take as it has potentially serious implications for the individual concerned and it is, therefore, important that we adopt a fair, consistent and considered approach. In particular, a referral to the police should only be considered in the most serious of cases, where it is possible that the incident concerned and the potential risk to patients may amount to a criminal offence.

10. It should also be emphasised that section 15 allows us to release any information to **any persons** and there may be a number of circumstances in which we could release such information lawfully to other bodies or individuals (for example, to a public inquiry). We can also disclose information about more than one individual to more than one organisation at the same time.

11. In some instances, the threat to patients will relate more to their health than to their safety. For example, in dentistry, serious mistakes may not be life threatening, but may affect the oral health of patients. In these cases, we can still share information under section 15.

Criteria

12. Any decision on making a disclosure will need to be determined by a balanced judgement taken in light of the circumstances of the individual case – caseworkers should also bear in mind any wider systemic issues which may need to be thought about when considering disclosure. This can be done by speaking to line managers and Assistant Directors and checking the Horizon Scanning Newsletter for any current and relevant systemic themes.

13. It is important to note that disclosure would not be appropriate for cases where we just make an adverse finding of fault. Disclosure under Section 15 should only be considered where we have identified an additional potential risk to the health and safety of patients. Below are some examples of the types of situations where we may want to disclose:

[4] An individual within a designated body (usually the doctor's employer) who is responsible for helping the doctor with their revalidation (affirming to the GMC that they are up to date with training and fit to practice).

- the specific incident giving rise to the complaint is so serious that there are justifiable concerns about the potential risk to other patients if the matter is left 'unreported' (for example, issues of significant professional incompetence) – this could also relate to concerns about record keeping;

- the incident is not an isolated one (for example, if there have been other complaints against the practitioner concerned where we have identified similar service failings, perhaps on a related theme);

- concerns relevant to the health and safety of a patient have been expressed about an individual by colleagues or other peers such as clinical advisers - even if colleagues or other peers have disclosed information to a regulator or other party, we can still formally disclose our concerns as well;

- an individual's ability, knowledge and experience in relation to the matter involved is significantly lacking;

- on significant clinical matters, the individual's attitude is inconsistent with relevant standards and established good practice – again this can relate to record keeping;

- the individual or body has not 'learnt lessons' from earlier complaints, is generally defensive (including failure to co-operate with the complaints procedure) and is likely to repeat similar serious failings;

- concerns relating to complaint handling and/or internal review/investigation of a specific incident – despite not being directly involved in care and treatment. (For example, we have disclosed information about clinicians under section 15 because of their failure to pick up on serious mistakes and/or take appropriate action as part of an internal review or investigation);

- the individual has failed to meet the relevant standards of conduct, for example in terms of honesty and integrity; for example, the falsifying of evidence;

- the individual has no on-going accountability to the NHS, so that the risk to patients from misconduct or poor practice is increased to an unacceptable level by a lack of suitable governance or supervisory arrangements, which may create a risk that further problems may not be identified; and

- if we find evidence to suggest that a practitioner has breached a conditional registration imposed by a professional body (for example, one of the sanctions available to both the GMC and GDC if they find that a practitioner's fitness to practise is impaired is to impose conditions on their registration for up to three years).

14. This list is not exclusive and it must be emphasised that a decision to disclose such information occurs only in a small number of cases.

15. If you are unsure about disclosing information under section 15 then the issue should be escalated through your line manager to an Assistant Director and advice sought from the Legal team.

Process

16. In cases where it is felt that disclosure under section 15 might be appropriate, the following action should be taken:

- Review the case risk rating on Visualfiles and ensure that the mitigation plan is up to date [Assessing risk in casework]. Whether or not the risk rating will need to be changed will be dependent on the individual circumstances of the case. However, both the risk rating and mitigation plans should be regularly reviewed throughout the life of the case.

- A separate history item noted on Visualfiles explaining the reasons why disclosure might be appropriate and cross-referencing to relevant evidence (including clinical advice).

- Details of the case escalated via line management to Assistant Director and then Director for consideration (and simultaneously copied to the Legal Team who should be invited to comment).

- Prior to the actual disclosure, consider telling the subject of the disclosure that we are proprosing to disclose information about them (unless there are urgent concerns which warrant immediate disclosure).

- If the case is considered suitable for disclosure then it should be referred to the Ombudsman, Managing Director or the Executive Director of Operations and Investigations for their agreement to disclose information.

- If a disclosure is made to a professional body (for example, GMC, GDC, NMC) then this should be noted on Visualfiles by ticking the '*referral to professional body*' box on the '*Case closure'* screen. This can be used at any point in the life of a case and should be noted at the time that a disclosure is actually made. It must not be used when a disclosure is only being considered.

- The letters containing the information for disclosure should be signed off at Assistant Director or above.

- In investigation cases, we usually share the relevant information at the same time as we issue our final report by copying an anonymised final report to the regulatory body or other organisation/person. However, the disclosure can be made urgently if necessary before the investigation is completed and the final report issued.

- In investigation cases where the person we are disclosing information about would not normally receive a copy of the final report (for example, if they were not listed as a 'named person') we should still send them a copy of the final report[5] in order to meet the obligation to inform the subject of the information being disclosed.

17. The exact sequence of events will be determined by the nature of the case. The key requirement is that any case which has the potential to result in disclosure under section 15 is identified and escalated at an early stage.

18. This link provides details of cases where we have disclosed information under section 15 and also contains example wording.

Compliance

19. The disclosure of concerns under section 15 is a process we follow when we consider it necessary. It is not a remedy for the complainant and there is no obligation on the organisation or person we have disclosed the information to, to tell us the outcome of our disclosure. Once we have made the disclosure, our involvement ceases. Therefore, there is no need to record the disclosure as a compliance item or create a compliance plan.

[5] s.15(1B) HSC.

Annex A

Extract from section 15 of the Health Service Commissioners Act 1993

15. Confidentiality of information

(1) Information obtained by the Commissioner or his officers in the course of or for the purposes of an investigation shall not be disclosed except -

(a) for the purposes of the investigation and any report to be made in respect of it,

(b) for the purposes of any proceedings for –

(i) an offence under the Official Secrets Acts 1911 to 1989 alleged to have been committed in respect of information obtained by virtue of this Act by the Commissioner or any of his officers, or

(ii) an offence of perjury alleged to have been committed in the course of the investigation,

(c) for the purposes of an inquiry with a view to the taking of such proceedings as are mentioned in paragraph (b),

(d) for the purposes of any proceedings under section 13 (offences of obstruction and contempt), or

(e) where the information is to the effect that any person is likely to constitute a threat to the health or safety of patients as permitted by subsection (1B).

(1A) …

(1B) In a case within subsection (1)(e) the Commissioner may disclose the information to any persons to whom he thinks it should be disclosed in the interests of the health and safety of patients.

(1C) If the Commissioner discloses information as permitted by subsection (1B) he shall -

(a) where he knows the identity of the person mentioned in subsection (1)(e), inform that person that he has disclosed the information and of the identity of any person to whom he has disclosed it, and

(b) inform the person from whom the information was obtained that he has disclosed it.

General Guidance: Disclosure of concerns about the health and safety of patients - Section 15 Health Service Commissioner's Act.

Case examples and example wording

Case examples of Section 15 disclosures

- HS-96487 (information shared in March 2012) – We shared concerns about a Practice Nurse to the NMC after she altered entries in a patients electronic GP records, deleted original entries and did not mark the substituted entries as retrospective. This was done following the Nurse becoming aware of a complaint made about her by the patient. The case was referred to in our report Listening and Learning.

- HS-91752 (June 2012) – We shared concerns about a GP to the GMC and their Responsible Officer after they repeatedly failed to comply with our recommendations.

- HS-99173 (November 2012) – We shared concerns about the Head of midwifery to the NMC because of failings in the handling of a complaint, including making knowingly dishonest statements to the complainant.

- HS-115930 (October 2012) – We shared concerns about an NHS Direct Nurse Adviser to the NMC for failing to properly assess a patient, failing to safely end the phone call and failing to act in accordance with NHS Direct's policies and the NMC Code resulting in a potentially avoidable death.

- HS-120304 (December 2012) – We shared concerns about a dentist to the GDC because he refused to accept our recommendation for financial compensation.

- HS-132263 & HS-139074 (March & October 2013) – Both cases (investigated separately) related to concerns about the same doctor who had failed to appropriately assess and manage risk for patients with mental health disorders. We shared our concerns with the GMC following receipt of the second complaint.

- HS-144917 (May 2014) – We shared concerns about four doctors to the GMC and a nurse to the NMC. One of those was a consultant not involved in the care and treatment but who led a Serious Untoward Incident investigation. We shared information with the GMC because we found that the consultant failed to identify serious clinical mistakes which brought his clinical competence into question.

Example wording for Section 15 disclosures

Disclosing information about a potential or actual threat to the health and safety of patients, can be included in the final investigation report, or the disclosure can

be made separately in a covering letter to the relevant organisation or other party. In either case, we should send a copy of our anonymised final investigation report to the relevant organisation or person. Suggested wording to go into both the body of an investigation report or the covering letter is detailed below:

Investigation report

Section 15(1)(e) and section 15(1B) of the *Health Service Commissioners Act 1993* allow us to disclose infomation obtained in the course of an investigation in the interests of the health and safety of patients, if the informtion shows that a person is likely to constitute a threat to the health or safety of patients.

In this case, we consider it appropriate to disclose information under section 15 for the following reasons:

- First, because our investigation has found serious failings in relation to Mr A's clinical record keeping.
- Secondly, because our investigation has raised serious questions about the standard of care and treatment provided by Mr A.
- Thirdly, because my investigation has identified serious failings in Mr A's handling of complaints.
- Finally, because Mr A's stated refusal to implement our recommendations raises serious questions about his understanding of and respect for the arrangements for investigating and resolving complaints about NHS bodies and individuals.

In our view, these four failings, taken together, mean that the actions taken by Mr A fell so far short of the relevant standards as to constitute a threat to the health and safety of patients. I also consider that the findings of this report and Mr A's response to our findings and recommendations raise questions about Mr A's fitness to practise as a dental professional, which should be addressed by the professional body with which he is registered, that is, the General Dental Council. We have therefore sent a copy of this report to the General Dental Council and asked them to consider our concerns about Mr A's fitness to practise.

Covering letter to organsation/other party

As you are aware, provision is made under section 15(1)(e) and section 15(1B) of the *Health Service Commissioners Act 1993* (the Act) to allow us to disclose information obtained in the course of an investigation in the interests of the health and safety of patients. Evidence gathered during the course of our investigation has, in our view, raised concerns for the safety of the patients of each of the following doctors and a nurse. We are therefore writing to you to disclose the relevant information which is set out in our final investigation report. A copy of the report is enclosed.

We are sharing this information with you because we consider that our findings on this investigation indicate that each of the doctors concerned failed to meet the standards of conduct set out in Good Medical Practice. They are, therefore, likely to constitute a threat to the health or safety of patients. Details of each doctor's failings and the relevant sections of Good Medical Practice are set out in our investigation report.

In accordance with the requirements of our legislation, we are also writing to each doctor, the organisation we have investigated and Mrs D to inform them of our decision to share this information with you. If you require any further information, or need assistance from us, please contact our investigator.

Covering letter to the subject of disclosure

I am writing to let you know that, on completion of our investigation we have decided to provide copies of our final investigation report to the GMC/NMC/GDC. This is because provision is made under section 15(1)(e) and section 15(1B) of the Health Service Commissioners Act 1993 (the Act) to allow us to disclose information obtained in the course of an investigation in the interests of the health and safety of patients. Evidence gathered during the course of our investigation has, in our view, raised concerns for the safety of the patients of four doctors and a nurse.

It is for the GMC and NMC to determine what action, if any, they take in response to the information contained in our report.