Parliamentary and Health Service Ombudsman

Service Model Policy and Guidance: general guidance

Version 12.0

Version: 12.0
Version Date: 3/7/2020

Contents

Introduction

1. The Parliamentary and Health Service Ombudsman's casework process is summarised in the Service Model. This guidance provides information about how our casework staff should operate in line with the Service Model.

2. The Service Charter contains 18 commitments about how we will deliver our service and what people can expect when they bring a complaint to us. The detailed information in the Service Model and this guidance helps us to deliver our service in line with the Charter commitments.

3. The intention of the guidance is to provide an additional layer of detail below the Service Model, with a particular focus on:

    - Requirements from the law (flagged as 'Legal requirement' in the text).
    - Requirements from our own policy (flagged as 'Policy requirement' in the text).

4. Those requirements set the framework within which our casework staff should operate. The guidance is not intended to prescribe the actions or process to be followed across all casework and in all circumstances. Many areas of casework require discretion and judgment and depend on the specific circumstances of the case. Any divergence from the stated requirements in the guidance should be recorded and explained on our case management system, Microsoft Dynamics (Dynamics 365).

5. The Supervision Model specifies the tasks and supervisory tasks that are required to complete PHSO casework. The Supervision Model and supporting guidance detail the minimal supervision requirements of staff processing casework. Staff must adhere to the Supervision Model at all times.

6. Please note that when the text of the guidance refers generally to 'caseworkers' this covers both 'caseworkers' and 'senior caseworkers'. The distinction between what the two types of caseworkers can do is set out in the Supervision Model and the Delegation Scheme.

7. This guidance document is a supplement to the main casework guidance and focuses on subject-specific or cross-cutting subjects. A casework reference library is also available which focuses on specific subject areas within our casework where separate guidance is required.

8. The guidance is a living document and will be updated on a regular basis.

9. The guidance is owned and maintained, on behalf of Operations, by the Quality Directorate.

10. If you have any feedback or questions about the guidance or related issues then please email: [redacted]

1. Assessing risk and when to escalate cases to the Ombudsman and Deputy Ombudsmen

Introduction

1.1 We use risk to refer to factors that in isolation or combined mean that a case should be managed and, in particular, supervised, differently. We use the term to cover the probability, threat of damage, or any other negative occurrence that is caused by external or internal vulnerabilities or influences that may be avoided or monitored through mitigation.

1.2 We assess risk because it enables us to carry out better quality casework that is handled appropriately dependent on the circumstances of the particular case. This includes having a case escalation process in place to allow us to identify cases the Ombudsman and Deputy Ombudsman should be made aware of, either for their oversight or for decision making.

1.3 We need to identify, analyse and manage risk continuously throughout the life of a case, in order to understand, control, avoid, remove, reduce or accept risk so we can carry out our casework effectively. Our risk process is dynamic and the rating level on a case can move between low, medium and high as we become aware of new risks, or the risk is removed.

1.4 Case risk should be managed by the individual allocated ownership of the case with whatever level of supervision or upward reporting is necessary as a result of the risk assessment.

1.5 The types of risks we should consider include the time the investigation is taking, the involvement of a potentially litigious body or person in jurisdiction, the profile of the case, the seriousness of the allegations and cases where our capacity to investigate is in doubt. Our casework risk categories are located in our Casework Risk Assessment Tool in detail, and some examples are provided at the end of this document.

1.6 We may from time to time decide that a particular group of cases, or a specific organisation, need to have a higher risk rating apply, for a temporary period of time. This could be for numerous reasons, for example the external profile of the case.

1.7 The process outlined below sets out our standard approach in undertaking an assessment of risk. There will be circumstances though when we decide a case should be a higher or lower level of risk for another reason. The process for considering this is detailed below.

What risks should we be capturing?

1.8 When considering risk we are looking at events or actions that are happening now, but are going to continue or worsen in the future or that are likely to happen in the future. For example, legal action currently being taken against

us, or the possibility a person will come to harm based on their current circumstances.

1.9 When considering what risks may occur in the future we will only include those applicable to the circumstances of the particular case. For example, if a complainant has a worsening health condition, such as arthritis, but this does not relate to their complaint, we would not add it as a risk.

1.10 We do not generally need to record risks that have already happened and should only reference past events as a risk if they are likely to have a future impact. **(Policy requirement)** For example, if a complainant has a complaint about our service upheld and brings a further complaint to us, there is already a risk they will be dissatisfied with our service.

1.11 If a risk we are attempting to mitigate occurs during our consideration of a case we should review the risk rating and decide whether it needs to change or is still applicable. **(Policy requirement)** For example, if there is a risk someone may lose their home as a result of an ongoing complaint, and this happens, we may decide we no longer need to record this as a risk. Of course, there may be a new risk as a consequence.

When to assess risk

1.12 The caseworker should ensure they proactively manage and monitor risk through-out the lifetime of the case. A risk assessment should be undertaken whenever a new potential risk is identified. **(Policy requirement)**

1.13 A formal risk assessment is also required at four points in the casework process.(**Policy requirement**):

- When we propose to investigate/decline to investigate (can we/should we look into your case)
- When we confirm the investigation (under investigation)
- When we share our provisional views
- When we decide to do further work following a complaint about our service or decision

1.14 The caseworker should ensure they accurately record all considerations of risk, and any proposed mitigations, on Dynamics 365. This includes the Intake Caseworker ticking that a risk assessment is required when passing a case for assessment and the caseworker ensuring that both a risk impact and likelihood rating are added to ensure an overall risk rating is generated.**(Policy requirements)**

1.15 Regardless of the risk type, the following questions must be considered when completing a risk assessment. (**policy requirement**):

- Is there a risk? (If so describe the risk in a short statement)
- What is the likelihood of the risk? (unlikely, possible or highly likely)
- What is the potential impact? (minor, moderate or critical)

- Do a number of risks taken together have a cumulative effect?
- How can we mitigate the risk?
- What do you expect the risk rating to be having taken mitigating action?
- What action do we take if the risk we have described happens?

Is there a risk?

1.16 There is no universal agreed list of what a risk has to look like, and the caseworker should consider whether an event or action constitutes a potential risk on a case by case basis. **(Policy requirement)**

1.17 We have five specific risk categories a caseworker should consider when deciding on a cases overall risk rating. **(Policy requirement)** Our Casework Risk Assessment Tool provides examples of what would usually constitute a minor, moderate or critical risk impact.

1.18 In most instances we will only consider a risk needs to be recorded if it directly links to the complaint made, the injustice claimed or outcome sought by the complainant. For example, distress and pain which the complainant says is a result of the surgery complained about going wrong, rather than ongoing issues as a result of an unrelated health condition.

1.19 We do not need to seek evidence a risk exists before considering it in our assessment, and can take account of information given to us by a complainant or organisation if reasonable to do so. For example, if a complainant tells us they are likely to lose their house if they do not receive monies owed, we do not need them to prove this.

1.20 The tool does not cover every category of risk which may be applicable, and the caseworker should take into account the specific circumstances of the case before deciding on an overall rating. **(Policy requirement)**

Recording risk

1.21 We should record a risk whenever one is identified, even when we know in advance this can be fully mitigated. **(Policy requirement)** This is to ensure we can demonstrate we have considered the impact of the risk and have a transparent plan in place to how we will deal with it.

1.22 If no risk is identified, a risk assessment should be recorded as low. The caseworker should write a brief summary explaining the reasons for the low rating. **(Policy requirements)** For example, stating there is no indication or evidence at this stage that a risk is present.

1.23 We should record any information we receive or discover that may not identify a risk at present, but will help us monitor whether one will develop in the future. **(Policy requirement)** For example, a complainant tells us they have a history of suicide attempts, but there is no suggestion that our action on their case could be a contributing factor. In this instance we may consider the

case risk rating to be low, but want to record this information in the risk section of our Decision Form and on Dynamics 365.

1.24 We may decide a case requires a higher risk rating for a limited period of time until we are sure an appropriate mitigation is in place. For example, following a change in approach to a type of case we may consider it requires a higher risk rating until we are sure those cases are being dealt with correctly.

What is the likelihood of the risk, and potential impact?

1.25 When assessing risk we should consider the severity of the risk (minor, moderate or critical) against the likelihood of the risk occurring (unlikely, likely or highly likely). **(Policy requirement)**

1.26 We should use our risk matrix to assist in determining an overall risk rating for the case of low, medium or high before and after mitigation takes place. We should use the post-mitigation rating when recording an overall level of risk on our Decision Form and on Dynamics 365, but should ensure the pre-mitigation rating is still referenced. **(Policy requirements)**

Is the case low or medium risk?

1.27 If following application of our risk matrix a case comes out as medium risk, the caseworker should consider further, in discussion with their manager if appropriate, whether the case requires a medium risk rating or can be graded low instead based on any other external factors. **(Policy requirement)**

1.28 The caseworker should consider if any external factors are applicable that may raise or lower the impact and likelihood of a risk occurring outside of the examples provided within the Casework Assessment Tool. **(Policy requirement)** For example, whether the allegations are serious, if the complainant is vulnerable, or if an advocate or other representative is available.

1.29 If a case relates to more than one category of risk we should record multiple risk ratings[1]. The overall rating for the case should usually be recorded as the highest level identified after mitigation takes place. **(Policy requirements)**

What if the rating doesn't seem right?

1.30 If in applying the risk matrix the caseworker feels the correct rating has not been generated for any reason, they should review the rating again and ensure they have covered all of the risk categories in their consideration. **(Policy requirement)**

1.31 If following this reconsideration the risk rating remains the same, and the caseworker still thinks it should be higher or lower, they should discuss the case with their manager. If their manager agrees the risk rating should be raised or

[1] See reference to cumulative risk ratings at section 1.35

lowered on the case, and an appropriate explanation to why should be recorded on the Decision Form and Dynamics 365. **(Policy requirements)**

Our risk matrix

<table>
<tr><th colspan="6">Risk and mitigation plan</th></tr>
<tr><td colspan="2" rowspan="2">Description of risk/s
(to be updated during the lifetime of the case)</td><td colspan="2">Impact</td><td colspan="2"></td></tr>
<tr><td colspan="2">Likelihood</td><td colspan="2"></td></tr>
<tr><th colspan="6">Risk matrix</th></tr>
<tr><td rowspan="6">Impact</td><td rowspan="2">3 - Critical</td><td>Medium</td><td rowspan="2">High</td><td rowspan="2">High</td></tr>
<tr><td>or Low</td></tr>
<tr><td rowspan="2">2 - Moderate</td><td rowspan="2">Low</td><td>Medium</td><td rowspan="2">High</td></tr>
<tr><td>or Low</td></tr>
<tr><td rowspan="2">1 - Minor</td><td rowspan="2">Low</td><td rowspan="2">Low</td><td>Medium</td></tr>
<tr><td>or Low</td></tr>
<tr><td></td><td></td><td>1 - Unlikely</td><td>2 - Likely</td><td>3 – Highly likely</td></tr>
<tr><td></td><td colspan="4">Likelihood</td></tr>
</table>

What if the case is high risk?

1.32 If the caseworker identifies a high risk case, this must be discussed with their manager as soon as possible. If the manager agrees with the risk rating then a mitigation plan should be completed and sent to an Assistant Director for review. (**policy requirements**)

1.33 If a case is high risk our escalation and allocation process will apply. Please see section 1.62 for details. **(Policy requirement)**

1.34 If a case is escalated for oversight by the Ombudsman or their deputies, the rating cannot be changed without their agreement. **(Policy requirement)**

1.35 The caseworker should also consider who else may need to be made aware of the case (and involved in mitigation planning). For instance colleagues in External Affairs (our Public Affairs staff, the press team or our Liaison Managers).**(Policy requirement)**

1.36 If there is an immediate risk, particularly to the welfare of individuals[2], it must be considered quickly and a decision taken on what action to take. (**policy requirement**)

[2] Our policies and guidance on unreasonable behaviour and making disclosures are available in this document.

Do a number of risks taken together have a cumulative effect?

1.37 If we identify several risks on a case, we should consider whether combined they should lead to a higher risk rating being applied. (**Policy requirement)** For example, if we identify four different categories of risk on a case and grade them all at medium, we should consider if overall the case should be rated high risk.

1.38 There are no specific criteria to when a rating should be raised for this reason, and the caseworker should consider this on a case by case basis **(Policy requirement)**. We should consider the following though in reaching a view.

- While there may be several categories of risk identified, do they all stem from one specific issue? If so, and it is likely we will only need to have one mitigation plan in place; we will not usually need to raise the rating.
- Are the issues completely unlinked and therefore risk needs to be managed over several areas? This may cause us to raise the risk rating.
- When considered all together, is the possible impact of the risk or the possibility of it occurring higher? This may be a reason to raise the risk rating.

How can we mitigate the risk?

1.39 A case assessed as being either high or medium risk must have a mitigation plan. (**Policy requirement**). 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 these four outcomes:

- Remove (Our action can prevent the risk from occurring)
- Avoid (By doing something different we can greatly reduce the likelihood of the risk occurring)
- Reduce (Our action cannot fully prevent the risk from occurring but can reduce the impact or the likelihood that it will.)
- Accept (Nothing can be done to mitigate the likelihood or impact of the risk)

1.40 Some suggestions to how we may mitigate specific categories of risk are available at the end of this document.

What do you expect the risk rating to be having taken mitigating action?

1.41 The caseworker should explain in the relevant section of the risk assessment record on Dynamics 365 if the mitigation action suggested has lowered the risk rating on the case. **(Policy requirement)**

1.42 If the risk rating has been lowered, the case can be progressed in line with the new rating. For example, if the case was medium risk and is now low then some caseworkers may require less supervision under our model.

1.43 Taking a mitigating action may not always lower the risk impact or likelihood. We should still take any action identified though if it is proportionate to the case and supports either the parties to the complaint or our staff in handling or managing the risk. **(Policy requirement)**

What should we do if the risk rating changes during the case?

1.44 If a new risk arises, or a previously identified area of risk is no longer of concern, we should review the risk rating on the case. We should also record details of the new assessment, including any changes to the risk level on the Decision Form and on Dynamics 365. **(Policy requirements)**

1.45 If the risk level changes we must consider whether the case requires reallocation based on our case categorisation process[3], or whether additional supervision is now required based on our Supervision Model. **(Policy requirement)**

What action do we take if the risk we have described happens?

1.46 It is understood that despite all possible mitigation, a risk may still occur. This section of the risk assessment form on Dynamics 365 should therefore be used to explain what should happen if it does. This could include details of who should be contacted to help manage the risk, for example through our disclosure policies.

Categories of risk and how we may mitigate them

People (including the threat of harm to self or others)

1.47 This category covers the physiological or psychological harm that an individual is either currently experiencing which is likely to continue or get worse or that they may experience in the future. This includes complainants who are or become terminally ill.

1.48 The type of mitigation we put in place in these instances will depend on the circumstances of the case. If a complainant is terminally ill we should consider prioritising their case for allocation.

1.49 This category would also cover risks where a person involved in a case has threatened harm to themselves or others. In these instances there would not need to be a link between the complaint raised and any action threatened in order for this to be recorded as a risk.

1.50 If a person threatens to harm themselves or others we should consider making a disclosure to a suitable person[4]. **(Policy requirement)** Sometimes a threat may relate directly to our proposed action on a case, for example, a suggestion someone may harm themselves if we do not uphold their case. In these

[3] Our criteria for casework categorisation are available in our main guidance.
[4] Further information on our disclosure policies is available in section 3 &4

circumstances we may decide to mitigate the risk by making a suitable person aware before sharing our decision such as an advocate.

Financial risk (including loss or misuse of information)

1.51 This category covers the financial loss a complainant is already experiencing which is likely to continue or get worse. For example, someone being unable to work leading to mounting financial issues. It also covers financial losses that may happen in the future. For example, a charging order not being lifted meaning a house will have to be sold in the future.

1.52 We may find it difficult to mitigate a current or future financial loss for a complainant prior to deciding if we will uphold the complaint or make formal recommendations. In some circumstances, especially if the complainant is vulnerable, it may be possible and appropriate to contact an organisation for their assistance. For example, asking them to extend a deadline for payment until our decision has been concluded, or if we decide not to uphold a complaint, asking if they would consider putting a payment plan into place to pay back any monies owed.

1.53 This category also covers the loss or misuse of information. In these instances we do not need to consider the likelihood this will happen, and will generally only record a risk if information actually does go missing or is misused.All information breaches should be reported to our Information Security Manager. **(Policy requirement)**

1.54 The mitigation in these circumstances will usually be to ensure any information shared incorrectly is destroyed or retrieved as soon as possible, and we prevent it being shared more widely. In these instances we may also wish to consider if there is a separate future risk to our reputation in this information being shared. A mitigation plan for this may be discussing what has happened with the complainant or the Information Commissioner as soon as possible.

Reputation/Political (including media coverage)

1.55 This category is wide-ranging and covers any threat that could be a risk to our reputation, for example, a campaign through either a pressure group or national newspaper. It also includes any involvement of an Member of Parliament (MP) in a complaint.

1.56 The mitigation for this category would be entirely dependent on the specifics of the risk and the individual case. It is likely with this category though that we may need to mitigate both a current and potential future risk. For example, a local media campaign may be a current risk, but the fact the campaign may get picked up by the national media could be a future one.

Our Service

1.57 The service category covers any risk associated with a complaint about our service or where we have previously received a complaint about our service, regardless of the action we then took.

1.58 In order to determine the risk rating for this category the caseworker should review any cases the complainant has brought to us previously and confirm whether they have made a complaint to us, and if so what the outcome was. **(Policy requirement)**

1.59 Any complaint about us that cannot be resolved through the management line should be escalated to the Review and Feedback Team in line with their processes. **(Policy requirement)**

Legal

1.60 Our legal risk category generally refers to the threat or undertaking of legal action against us. It also includes the use of legislation as a standard in our casework and any complaint raised with us by a legal representative.

1.61 Any serious threat of legal challenge, pre-action protocol or claim such as judicial review must be referred to the Legal Team as soon as received. **(Policy requirement)**

High risk escalation process

1.62 We have specific processes for handling cases considered to be high risk under this policy to ensure they are given the relevant level of senior level oversight. These cases will always be allocated to a Senior Caseworker if the risk is identified early on.

1.63 When it is agreed a case is high risk after mitigation, the caseworker should ask for it to be assigned to either the Ombudsman, or one of their deputies, for oversight. **(Policy requirement)**

1.64 The most high profile cases (in particular those who involve systemic issues or a high degree of complexity) are allocated to the Ombudsman. As their capacity is reached, cases are allocated to their deputies.

1.65 The caseworker will continue to be responsible for progression of the case, with support from their manager, and the relevant Assistant Director – Casework as appropriate. The Assistant Director – Casework for Senior Caseworkers retains overall responsibility for high risk cases.

1.66 Cases are assigned via the high risk case assurance meeting, and a template should be completed, and submitted to the Assistant Director – Casework for Senior Caseworkers for inclusion and allocation. **(Policy requirements)**

1.67 Decisions on allocation must include consideration of any declared conflicts of interest. **(Policy requirement)** This is likely to include not allocating a case to the Director of Legal and Professional Services in their deputy Ombudsman capacity if legal advice is a key factor in the case decision.

1.68 The level of involvement by the Ombudsman or their deputies will depend on the circumstances of the individual case, but the caseworker and their manager should seek their involvement on any strategically important issues, and in the planning of any investigations. **(Policy requirement)** Caseworkers can arrange planning meetings with the senior decision maker through the executive office using the template above, and the briefing they prepare.

1.69 As part of the oversight process the caseworker may need to meet with the Ombudsman or their deputies. For such meetings they should be accompanied by their manager, or Assistant Director. The caseworker is responsible for making a record of the meeting and seeking approval of these notes afterwards. **(Policy requirements)**

1.70 Where the Ombudsman or his deputies make a casework decision (such as a decision to decline to investigate or a decision to approve a final report) that decision will be recorded on the cover note to the briefing paper, and stored on Dynamics 365. **(Policy requirement)**

1.71 Any approval received of the meeting notes, or of a decision, must show the decision maker has read, considered, and approved the contents. This approval must then be stored on Dynamics 365. **(Policy requirements)** Evidence of approval or consideration can be by way of a saved email trail if saved to the case.

1.72 The caseworker should send monthly updates ahead of each high risk case assurance meeting until the senior decision maker agrees otherwise, or work on the case is complete. **(Policy requirement)**

Conflicts of interest

1.73 Conflicts of interest are a relevant consideration in our risk assessment of a case as a conflict (if not identified or acted upon) could be a risk to our ability to carry out our function.

1.74 HR provides policy and guidance on identifying and declaring personal conflicts of interest. Where a conflict of interest exists in relation to the staff involved in a case then this must be reflected in the risk assessment and appropriate mitigation put in place.

1.75 Consideration of potential conflicts of interest should also take into account the declared interests of Board Members and other senior staff, where relevant.

1.76 Where a conflict of interest is identified on a case it must be documented on Dynamics 365, either as part of a mitigation plan or in a separate document if

there is no mitigation plan (for example, if a conflict is identified but the case remains low risk).

1.77 The completion of a risk assessment means that the member of staff has considered all relevant risk factors, including conflicts of interest.

2. Unreasonable behaviour policy

Policy statement[5]

2.1 We are committed to dealing with all people fairly and impartially and to providing a high-quality service. In order to do this it is important that we are able to communicate with someone bringing a complaint to us so we can make sure we fully understand it. We therefore do not normally limit the contact that people have with us.

2.2 We do not expect our staff to tolerate any form of behaviour that could be considered defamation, abusive, offensive or threatening or as defined by the Equality Act 2010, harassment or discrimination. Or that becomes so frequent it makes it more difficult for us to complete our work or help other people. We will take action under this policy to manage this type of behaviour and this applies to all contact with us including the use of social media.

2.3 We will make reasonable adjustments in line with the Equality Act 2010 in order to remove barriers to accessing our service. It is important to us though, that we provide a safe environment for our staff to work in, which may mean we decide to restrict how someone can contact us.

2.4 If we consider a person's behaviour is unreasonable we will tell them why and will ask them to change it. If this behaviour continues, we will take action including deciding whether to restrict the person's contact with us. This decision will usually be taken by an Assistant Director[6].

2.5 We will usually only take action to restrict someone's contact with us after we have considered whether there are any other alternative approaches we could make to prevent unreasonable behaviour from occurring. 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, email only);
- only allowing contact with a specific member of staff or at specific times;
- asking the person to enter into an agreement about their future behaviour; and/or
- actions designed to specifically meet the needs of the person.

2.6 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.

[5] 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.
[6] All decisions in this policy can also be agreed by members of staff who hold roles at a more senior level than referred to.

2.7 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.

2.8 There will be occasions where we decide that a person's behaviour is so extreme that it threatens the immediate safety and welfare of our staff or others. In these instances we will consider stopping all contact immediately, reporting what has happened to the police or taking legal action. In such cases, we may not warn the person before we do this.

What is unreasonable behaviour?

2.9 Unreasonable behaviour is difficult to define and will usually depend on the situation of the individual concerned. It can occur in a variety of circumstances including in person, on the telephone, in written correspondence or on social media (see paragraph 2.72).

2.10 Any behaviour that makes someone feel uneasy, uncomfortable, distressed, anxious, unsafe, intimidated, degraded or humiliated is likely to be considered unreasonable and action can be considered under the policy in these instances. Examples include behaviour that a staff member considers defamatory, abusive, offensive or threatening in nature or harassment or discrimination as determined by The Equality Act 2010.

2.11 We should also consider taking action under the policy where a high frequency of contact causes a disruption to the service we provide. For example, a series of disruptive calls which contain no abusive content may be suitable for action to be taken under this policy as much as a single call which contains a specific threat.

2.12 If at any stage we consider a person's behaviour poses an immediate threat to the health, welfare or safety of staff then we should decide whether more immediate action is required. Further information about what action to take is available at paragraph 2.60.

<u>Considering equality issues in deciding whether to take action under the policy</u>

2.13 The staff member must take into account any equality issues that may affect a person's behaviour before deciding whether to take action under the policy. This should include reviewing any reasonable adjustments currently in place and deciding whether any further steps could be taken to manage the person's behaviour.

2.14 Any changes to reasonable adjustments should be recorded on Dynamics 365 and confirmed in writing to the complainant. Guidance on making and applying reasonable adjustments can be provided by the Equality, Diversity and Inclusion Specialist.

2.15 If we decide to make further reasonable adjustments we should clearly record what we have agreed to do in the reasonable adjustment section on the

complainant's Dynamics 365 record, the task section of the complainant's current case and confirm in writing to the complainant. **(Policy requirement)**

2.16 If the staff member considers further adjustments cannot be made to support the person, or their request for adjustment is unreasonable, then the reasons for this decision must be recorded on Dynamics 365 and discussed with the Legal Team. If the staff member has concerns about deciding that a requested adjustment is not reasonable, they must consult their manager, and also the Legal Team if appropriate. **(Policy requirements)**

2.17 A staff member can still take action under this policy even if a relevant equality or diversity issue is identified. They must take account of any reasonable adjustments agreed in deciding what action to take. **(Policy requirement)** For example, a dyslexic complainant may only want telephone contact. We may therefore decide to limit their contact to one person, rather than restrict all telephone calls to us.

Recording unreasonable behaviour

2.18 The staff member should log full details of any behaviour they consider to be unreasonable on the tasks section of Dynamics 365. This record should include details of why they consider the behaviour is unreasonable and details of, for example, any offensive terms used. **(Policy requirement)**

2.19 The staff member should record the exact language used in the contact 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 the way they spoke and how they acted. They should also create a new record for each telephone call to capture the frequency of the contact. **(Policy requirement)**

The process

2.20 Staff members should complete each stage of the process below before moving to the next and should only take further action if the person's behaviour continues to be unreasonable. **(Policy requirement)** A diagram of the process is also available in annex A.

- 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 as an alternative method of communication.
- Issue a warning with the agreement of a manager and provide details of our policy.
- Escalate to an Assistant Director to consider applying the policy.

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

2.21 The staff member who has experienced the unreasonable behaviour should usually be the one to challenge it. This is because they are in the best position to explain why the person's behaviour is unreasonable.

2.22 The staff member should tell the person involved that they consider their behaviour unreasonable, explain why, and give them the opportunity to stop. (This explanation can, if necessary, be given at the same time as a warning about the potential application of this policy.) They should also ask the person at this time if there is a way we can adjust our service to help them. **(Policy requirements)**

2.23 If for any reason the staff member feels uncomfortable in challenging the person's behaviour at the time, or is concerned their personal safety is at risk (particularly if the behaviour is threatening or occurs in a face-to-face setting), they should record any details of the person's behaviour and discuss what happened with their manager as soon as possible. The staff member can still contact the complainant, taking into account any reasonable adjustments in place, to discuss their behaviour after the incident if appropriate.

Examples of when and how to challenge unreasonable behaviour

2.24 If a person uses offensive language during a telephone call the staff member involved should explain to the person that their language is unreasonable and ask them to stop. If the person refuses to comply with that request the staff member should politely end the call. A record should be made on Dynamics 365 of what has happened and the telephone call should be discussed with a manager.

2.25 If a person uses offensive language in letters or emails, the staff member should explain in their next written response to the person that the language they have used is unreasonable and ask them not to repeat this in future correspondence. Examples of sample letters are available in annex B.

2.26 If a person persistently makes repeated telephone calls without legitimate purpose (for example, to ask about progress on their case when they have recently been given that information) the staff member involved should explain to them that their behaviour is disruptive and is preventing work on their case and others. They should ask the person to stop doing this. If the person refuses to comply with the request then in the short term 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 the behaviour continues the staff member must take action under the policy and should not continue to just terminate calls. **(Policy requirement)**

2.27 If a person 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) the staff member should ask, in their next

contact with the person, that they limit the amount of correspondence sent to us.

2.28 If a person visits the alternative working premises of an employee with the purpose of engaging with them on their work i.e. a clinician who works part-time for us is contacted by a complainant whilst they are working in their alternative role. The staff member should explain this is inappropriate and ask the person to contact them while they are in the office. The incident should then be shared with the relevant caseworker, and consideration given to action under the policy.

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

2.29 If a person displaying unreasonable behaviour has an advocate, the staff member should approach them as soon as possible to ask for assistance in understanding and managing the person's behaviour.

2.30 If the person does not have an advocate, the staff member should, if appropriate, suggest they get one and provide details of a suitable provider. This may be particularly suitable in cases where there are equality considerations. **(Policy requirement)**

Issue a warning with the agreement of a manager[7] and provide details of our policy

2.31 A warning will normally be given before the policy is applied. This is different to telling the person their behaviour is unreasonable. The staff member will usually have already told the complainant why their behaviour was unreasonable and given them the opportunity to change.

2.32 The staff member should consider the most appropriate way of giving the warning, whether this is telephone, email or by post, taking into account any reasonable adjustment in place. The staff member should also record the warning in the alerts section of the person's Dynamics 365 record. This must include a summary of the reasons for the warning, the date and the manager it was discussed with. **(Policy requirement)**

2.33 If the warning is communicated over the telephone the staff member should also send the person concerned either a copy or a link to the policy statement via email or writing (paragraphs 1-8 above are available on PHSO's website). This should be accompanied by a brief letter, taking into account any reasonable adjustments in place, reiterating the warning and if appropriate a statement of our willingness to discuss a reasonable adjustment if helpful. **(Policy requirement)**

2.34 The staff member involved should usually deliver the warning as they are best placed to explain why the complainant's behaviour was unreasonable. Another staff member can do this though if appropriate. The warning should

[7] If the member of staff dealing with the case is a manager at grade 2 or above, then they do not need the agreement of their manager before issuing a warning.

explain what the behaviour was, why we consider it to be unreasonable and the likely consequences of any continuation.

2.35 The staff member should usually discuss the decision to issue a warning in advance with a manager. There will be occasions when a person's behaviour (usually during a telephone call) requires a staff member to issue a warning without being able to discuss the case with a manager first. In these instances the staff member should inform their manager as soon as possible after the event. **(Policy requirement)**

2.36 If a Member of Parliament and/or representative have been involved in the case, the staff member should tell the person that, if the unreasonable behaviour continues and we decide to apply our policy, that we will tell the MP and/or the representative. **(Policy requirement)**

2.37 If the staff member considers the person's behaviour is particularly serious (for example, there has been a specific and immediate threat made) a decision may be taken by an Assistant Director to apply the policy without prior warning. In that event, the staff member who authorises the application of the policy should contact the person immediately explaining the reasons for doing this. **(Policy requirement)**

2.38 The staff member should also consider whether the Security Officer[8] should be informed. This will mainly be relevant when the staff member feels threatened by the person's actions, for example a threat is made to come to our offices, someone's alternative working practices or a personal address.

Recording a warning on Microsoft Dynamics

2.39 The staff member should record the warning on the 'alerts' section of the customer record. They should enter details of the warning, the date given and the manager who agreed it. This will appear on a banner at the top of the case screen and on the customer record. Restrictions applied will only normally apply to an individual and therefore to their contact on any cases they have with us. The staff member will therefore need to specify if the restrictions only apply to one case. **(Policy requirement)**

2.40 Information about how to record a warning, decision and review on Visualfiles is available in Annex D.

Escalate to consider application of the policy

2.41 If the staff member continues to behave in a way that is unreasonable a request to apply the policy should be referred to an Assistant Director. The person making the request should ensure the request provides relevant details including those detailed below and is recorded on the task section of the complainant's Dynamics 365 record: **(Policy requirement)**

- nature and frequency of the behaviour;

[8] The relevant Security Officers for the purpose of this policy are our Facilities Managers.

- steps taken so far to manage the behaviour;
- information about the complainant's needs and circumstances, including equality and diversity considerations that may impact on the requirements/conditions applied;
- proposed requirements/conditions; and
- duration of proposed requirements/conditions

2.42 In deciding whether to apply the policy and refer to an Assistant Director the staff member will consider the above points and record on the task section of Dynamics 365; **(Policy requirements)**

- The requirements/conditions for the person to follow in order to manage their behaviour.
- Whether there are any equality or diversity considerations that may impact on the requirements/conditions agreed.
- Advice and support to any staff members who receive contact from that person.
- Date for review of requirements/conditions.
- Responsibility for handling requests for review of requirements /conditions.

2.43 The staff member should record the outcome of the referral on Dynamics 365 and detail the reasons why it has been agreed or not agreed that the policy should be applied. This should include whether restrictions need to apply to any other existing enquiries, reviews, investigations or information requests that the person has with us. **(Policy requirements)**

2.44 If it is decided that the policy should not be applied then the Assistant Director who considers the request, in consultation with the staff member should decide how to manage contact from the person in the future and record this on Dynamics 365. **(Policy requirement)**

2.45 If it is decided the policy should apply, the Assistant Director considering the request, in consultation with the staff member should agree how to restrict the person's contact with us. In doing this they should balance the interests of the person with the duty to protect the health, safety and welfare of staff. **(Policy requirements)**

2.46 Possible actions include:

- requesting contact in a particular form (for example, emails 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.

2.47 When applying a restriction the Assistant Director considering the request should set a date when it will be reviewed. This date should be recorded on

Dynamics 365. This will not be more than 6 months after the restrictions are imposed. **(Policy requirement)**

2.48 The staff member applying the restrictions should contact the person and explain:

- the reasons for the decision;
- the requirements/conditions the person must follow and any adjustments that can be made to assist with 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.

2.49 The staff member should preferably make this contact by telephone. If they are aware that the person has a preferred method of communication or a reasonable adjustment in place regarding communication methods then contact should be made this way instead. This contact must be followed up in writing taking into account any reasonable adjustments in place. **(Policy requirements)**

Recording the application of the policy and restrictions on Microsoft Dynamics

2.50 The staff member should record that the policy has been applied and the restrictions under the 'alerts' section of the customers Dynamics 365 record. They should also include details of the Assistant Director who approved the decision and the date the restrictions should be reviewed. **(Policy requirement)** This will now appear on a banner at the top of the case screen and on the customer record. The staff member will need to specify if only applying the policy to only one of multiple cases.

2.51 The staff member should set up a task to alert them when the policy is due for review. If they are no longer the staff member dealing with the person on this date then they should contact the staff member currently dealing with the person to inform them a review is due. If the staff member leaves the organisation, their manager is responsible for conducting a review. **(Policy requirements)**

2.52 The staff member who is currently dealing with the person (or their case) is responsible for keeping the case record updated about the application of the policy. This includes where restrictions on contact are altered, varied or removed. **(Policy requirement)**

What if contact restrictions that have been applied are not complied with?

2.53 If a staff member receives a telephone call from a person who has been informed they cannot contact us this way, they should explain the restriction to

the complainant. They should politely ask the person to contact us using an alternative method or via an advocate. The call can then be terminated. **(Policy requirement)**

2.54 If a staff member receives a letter or email from a person who has been informed they cannot contact us this way, then they should explain this restriction to the complainant (this can be in writing if appropriate). They should then ask the person to contact us using an alternative method or via an advocate.

What if unreasonable behaviour continues after the policy is applied?

2.55 If the person continues to behave unreasonably after the policy has been applied, then the manager of the staff member currently dealing with the person should decide whether further restrictions are required. They should ensure that any changes made are recorded on Dynamics 365 as soon as possible. **(Policy requirement)**

2.56 An Operations Director can decide to terminate contact with a person completely if appropriate (which would also have the effect of closing or discontinuing any assessment, investigation or review consideration currently ongoing). The intention of this policy though is to manage challenging behaviour so we can continue to work on cases. This should therefore only be considered in rare circumstances. If the decision is made to do this then this should be recorded on Dynamics 365. **(Policy requirement)**

2.57 If the decision is made to terminate contact completely, then the manager of the staff member currently dealing with the person should write to the person, taking account of any reasonable adjustments, outlining our decision to terminate contact and what this will mean for any outstanding complaints. Any action taken must be recorded on Dynamics 365.

Complaints about decisions to apply the policy

2.58 The Review and Feedback Team can consider complaints about whether the policy has been applied in line with this guidance. If the process has not been followed correctly, the Review and Feedback Team should pass the case back to the manager who applied the policy and ask for it to be reconsidered. The outcome should be recorded on Dynamics 365. **(Policy requirement)**

2.59 If the complaint concerns our decision to apply the policy, the complaint should be forwarded to the manager of the manager to review the restrictions. The member of staff carrying out that review must issue a written decision to explain the outcome and record the decision on Dynamics 365. **(Policy requirement)**

Behaviour that poses an immediate risk

2.60 There will be exceptional cases where we consider a person's behaviour poses an immediate threat to the health, welfare or safety of staff members. In

these cases an Assistant Director may approve action to be taken without prior warning, including terminating all contact. They may also consider other suitable action such as police involvement. **(Policy requirement)**

2.61 The staff member taking this action should clearly recording what action has been taken on Dynamics 365 and the security officer should be notified. **(Policy requirement)** A risk assessment template and guidance on completing a risk assessment are available (see Annex C for details).

Modification of behaviour

2.62 If a staff member considers the person has modified their behaviour before the review date to the extent that existing restrictions should not apply, a proposal to remove or modify the restrictions can be agreed by an Assistant Director.

2.63 If restrictions are removed on a person's contact with us before the review date set the staff member should contact the person to explain this. At this time they should also make it clear to the person that if their previous behaviour resumes this could lead to restrictions being imposed again or further restrictions applied. **(Policy requirement)**

Deciding whether to continue applying the policy at the review date

2.64 The staff member who currently holds the case has the responsibility for ensuring a review is conducted (including cases that are held by the Review and Feedback Team).This is because they are best placed to comment on whether the person's behaviour has changed and restrictions should be lifted. **(Policy requirement)**

2.65 Before the review date the staff member should discuss the case with their manager and pass it to an Assistant Director to review their recommendations. **(Policy requirement)**

2.66 The person reviewing the case should take into account the evidence and reasons for making the original decision, and any evidence of the person's subsequent behaviour. They should also seek comments from appropriate staff, including those affected by the behaviour, and consider the effectiveness of any adjustment already made. **(Policy requirement)**

2.67 If the person reviewing the case decides not to extend the original restrictions for a further period, the conditions imposed will lapse. This decision should be recorded on Dynamics 365 and the alert should be removed from the case.

2.68 If there is continuing contact with the person, the person reviewing the case should write to them explaining the decision. If the person is not in regular contact then contact does not need to be re-established to tell them about the decision. The decision should then be shared if and when they make contact again.

2.69 If the person reviewing the case does not extend the original decision and the unreasonable behaviour occurs again at a later point they can decide to enforce the previous restrictions again without going through the warning stage.

2.70 If the person reviewing the case decides to extend the original decision, they should set a further period during which restrictions should apply up to a maximum of twelve months. When this expires, a further review should be conducted. **(Policy requirement)**

2.71 The review of the application of this policy should be recorded fully on Dynamics 365 by (or on behalf of) the person carrying out the review. The alerts box should then be updated to reflect any decisions made. **(Policy requirement)**

Social media[9]

2.72 We generally consider unreasonable behaviour on social media (for example, Facebook or Twitter) to be when a person is abusive, offensive makes personal threats or defamatory comments or repeatedly references an individual member of staff. We should not usually take action under this part of the policy if the comment is a general criticism of our organisation or service.

2.73 If a person displays unreasonable behaviour on social media then this policy can be used to try to manage it. In these circumstances the staff member responsible for responding to the person should not continue to respond online, in order to prevent personal or confidential information (either about a case or about a member of staff) being disclosed or publicised further. Instead they should follow the process, detailed earlier in this guidance, as if the unreasonable behaviour had been exhibited by telephone, email or letter etc.

2.74 If a social media post about a specific member of staff is found online, then this should be referred to the relevant staff member's manager, human resources, the Digital Communications team and our Data Protection Officer.

2.75 A screen shot of the contact should be emailed to our Data Protection Officer, including any information held about the time and date the message was posted, any webpage address and identifiers such as twitter handles, or usernames. This should ideally be accompanied by a note of the impact this has had on the named person, and their work, and an explanation if this is the first time this has occurred.

2.76 The manager should inform the staff member and take responsibility for agreeing what action to take, working with the Digital Communications team, Information Assurance and, if appropriate, the Legal Team. **(Policy requirements)** The following options can be considered:

[9] Please also see our Social Media policy.

- support for the employee (including employee assistance programme);
- asking the person who made the post to remove it; (discuss this with the Digital Communications team first)
- asking the Digital Communications team to report the person to the social media platform (if the behaviour persists);
- seeking advice from the Legal Team.

Contact received on staff member's personal social media

2.77 Most comments we receive on social media will be made to our corporate accounts. Action can be taken under this policy though in relation to contact received from a person that is sent directly to a member of staff's personal social media account.

2.78 If a staff member receives contact through social media from a person who is currently, or has previously, used our service then they should raise this with their manager. The staff member should not respond to the contact or acknowledge the person has a case with us, as this may be considered a breach of data protection. **(Policy requirement)**

2.79 If the contact is abusive, offensive, makes personal threats or defamatory comments the staff member should report it to their manager as soon as possible. The manager should then consider whether action is required under this policy. **(Policy requirement)**

Further complaints and information requests

2.80 Restrictions under this policy should usually be applied to an individual. We can still decide to apply restrictions on a case-specific basis if appropriate. **(Policy requirement)** This should be considered on the individual circumstances of the case.

2.81 If a person who has had restrictions applied under this policy seeks to make a fresh complaint, the staff member should consult an Assistant Director for a decision on how to respond to that further contact.

2.82 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 Assistant Director should be consulted for advice as well as our FOI/DP and Legal Teams. **(Policy requirement)**

Variation of these procedures

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

3 Disclosure of concerns about the health and safety of patients – section 15 Health Service Commissioner's Act 1993

Legislation

3.1 Section 15(1)(e) of our health legislation[10] gives us the power to disclose information to any person we consider relevant, if it is clear there is a likely threat to the health and safety of patients. (**Legal requirement**) Therefore if, during our consideration of a health case[11], we discover any information that would indicate a likely threat, we should consider whether disclosure of those concerns might be appropriate.

3.2 Once we have made the disclosure, the law[12] says we must ensure both the person supplying us with the information, and the subject of that information are told we have made a disclosure, and who we have made it to. **(Legal requirement)** The relevant section from the legislation is at Annex E.

Background

3.3 We should consider making a disclosure in any situation where we have reliable evidence that leads to us having concerns about the actions or behaviours of an individual or organisation.

3.4 However, whilst our legislation gives us a legal basis to disclose information in certain circumstances, we must consider the data protection principles and requirements set out by the Data Protection Act 2018 and the General Data Protection Regulation when undertaking any such disclosure exercise. **(Legal requirement)**

3.5 Confidentiality should be maintained so far as possible and the principle of data minimisation (only disclosing information that is necessary, adequate and relevant to achieve our purpose) should be followed. Please consult the Data Protection Officer if you have any queries. **(Policy requirement)**

3.6 Before deciding to make a disclosure though we must ensure we have sufficient evidence to conclude there is a likely threat to the health and safety of patients. We must also make sure any disclosure we make is proportionate in relation to what has happened or might happen. **(Policy requirements)**

3.7 If we do decide to make a disclosure then this should always be to a relevant person or organisation that has the powers and responsibility to handle the information provided and take action. **(Policy requirement)**

[10] Health Service Commissioners Act; 1993 section 15(1)(e)
[11] 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. This therefore may include information obtained in intake, assessment or review stage.
[12] 1993 Act, section 15 (1)(c)

3.8 We should also only disclose the minimum amount of information needed in order to respond to the threat and should not provide details of any case we are considering that is linked to the disclosure, unless directly relevant. **(Policy requirement)**

3.9 We should disclose information at any point we consider it necessary. We do not need to wait until the end of a case but should ensure we take a fair and reasonable approach. **(Policy requirement)**

3.10 We do not have the same powers under our parliamentary legislation, and therefore any consideration of whether to disclose information for these cases must be considered under our disclosing information about risk policy[13]. **(Policy requirement)**

Disclosing information concerning the actions of a clinician

3.11 It is likely that most of the disclosures we make under section 15 will concern the actions of clinicians. This has potentially serious implications for the individual concerned and therefore it is important that we are fair and consistent in deciding whether to make a disclosure.

3.12 Before making a disclosure we should consider whether our concerns could instead be dealt with through discussions with the employing or supervising NHS organisation involved in the complaint as part of our usual casework process. We should also consider that findings and recommendations made during an investigation will already be shared with the responsible organisation. **(Policy requirements)** If we partly or fully uphold a complaint about a doctor, then an anonymised version of the final report will also be shared with their responsible officer[14].

3.13 There will be occasions when we decide information should be reported to a regulatory or other external organisation or to other individuals. For complaints about clinicians this is likely to be their regulatory organisation. (We do not refer individuals to their regulatory organisation or employer; we share information with them.)

3.14 Disclosures to the General Medical Council, National Midwifery council, General Dental Council and Health Care Professions Council should be made through our contact points. **(Policy requirement)** Their details are held by our Lead Clinicians.

3.15 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

[13] Our Disclosing information where there is a risk to the health and safety of a complainant or others policy is available in section 4 of this guidance.
[14] An individual within a designated organisation (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).

threatening, but may affect the oral health of patients. In these cases, we can still share information under section 15.

3.16 We can decide to make disclosures to the police, but should only consider doing so in the most serious of cases. This is likely to be where the incident concerned and the potential risk to patients is likely to amount to a criminal offence.

Disclosing information concerning the actions of others

3.17 Section 15 allows us to release information to **any persons** and there may be a number of circumstances in which we could release 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.

3.18 If the caseworker is unsure about whether information can be disclosed under section 15 then they should escalate their concerns to a manager and the Legal Team before taking any action. In circumstances where a disclosure needs to be made urgently and a manager or the legal team is not available, the staff member can still make a disclosure. They must discuss the case with a manager as soon as possible though following the disclosure being made.**(Policy requirement)**

When a disclosure may be appropriate

3.19 The decision to make a disclosure will need to be determined by a balanced judgment taken in light of the circumstances of the individual case. We should not be making disclosures just because we are making an adverse finding.

3.20 We should also consider whether there are any wider systemic issues that need to be looked at before making a disclosure. **(Policy requirement)** For example; we receive several complaints in relation to a cancer unit at a particular hospital that may indicate a wider issue. This can be done by speaking to Managers and Assistant Directors.

3.21 Below are some examples of the types of situations which we may decide are serious enough to warrant making a disclosure:

- 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, such as inaccurate information in the medical records;

- 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);

- an individual's ability, knowledge and experience in relation to the matter involved is significantly lacking or their attitude is inconsistent with relevant standards and established good practice – again this can relate to record keeping;

- the individual or organisation 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 organisation (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).

3.22 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.

The process

3.23 Where it is felt that a disclosure under section 15 might be appropriate, the following steps should be completed. **(Policy requirements)**

3.24 The caseworker should discuss the case with their Manager to decide whether a disclosure may be appropriate. They should then record this discussion in detail on Dynamics 365 and cross-reference the relevant evidence and advice (including clinical).

3.25 Where we are looking to disclose information about a clinician to their regulator, we should consider seeking clinical advice to establish the severity of the failings or concerns identified and whether action already taken to learn from the incident is sufficient. If a caseworker would like to seek advice on this, they should contact one of our lead clinicians.

3.26 The caseworker should review the case risk rating on Dynamics 365 and ensure that any mitigation plan is up to date. Whether the risk rating needs to be changed will depend on the individual circumstances of the case, however both the risk rating and any mitigation plan should be regularly reviewed. (**Policy requirement**)[15].

3.27 Details of the case should be escalated via line management to an Assistant Director to decide if a disclosure should be made (and simultaneously copied to the Legal Team who should be invited to comment) in line with the Delegation Scheme. The letters containing the information for disclosure should also be signed off at this level or above.

3.28 The caseworker should consider telling the subject of the disclosure that we are proposing to share information about them with a third party **before** doing so. There will be instances where this will not be appropriate, such as when a disclosure needs to be made urgently.

3.29 This approval should be clearly recorded on Dynamics 365. We should disclose the minimum amount of factual information needed to mitigate the risk to the minimum number of organisations. This includes limiting any case specific information we provide to what is necessary to explain the reasons for the disclosure. If a disclosure is made to a professional organisation (for example, GMC, GDC, NMC) then this should also be recorded on Dynamics 365.

3.30 We can make the disclosure by telephone or in writing. If we use email, we should ensure that the person we are disclosing information to 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, ensuring that documents are sent securely through Egress[16]).

3.31 If we have not already done so, we must ensure we meet our legal obligations by informing the person involved that we have made a disclosure and who we have made it to. We must then inform the person who provided us with the information that we have shared it. **(Legal requirement)**

3.32 The details of the disclosure, including the reasons why it was made, should be sent to the Change Delivery Team to add to the Section 15 disclosure registry.

3.33 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.

[15] The guidance for risk ratings is available in section one of this document.
[16] Further information is available at the following link: How to send a secure email in outlook using Egress

When to disclose cases and how

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

3.35 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[17] in order to meet the obligation to inform the subject of the information being disclosed. **(Legal requirement)**

3.36 There will be occasions where we decide not to investigate a case, or are still considering what action to take, but still want to disclose information. The same process applies, but we should be careful to ensure we only share information about the complaint that is necessary in order to make the disclosure.

3.37 Disclosures should usually be made at the same time we issue our decision. A disclosure can be made before then though if necessary. We must ensure we meet our legal obligations by informing the person involved we have made a disclosure and who we made it to. As well as informing the person who provided us with the information that we have shared it. **(Legal requirement)**

Section 15 cases where there is an immediate risk to a patient

3.38 There will be circumstances where there is an immediate risk to the health and safety of a patient which requires us to disclose information straight away.

3.39 In instances where an Assistant Director or above is not available, an Operations Manager,[18] or Senior Solicitor, 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).

3.40 It is unlikely that a staff member will have to act alone when considering or making disclosures but, if there is a serious and immediate threat to an individual and an Assistant Director, Operations Manager, Senior Solicitor cannot be contacted immediately, a staff member may make the disclosure without prior authorisation. **(Policy requirement)**

3.41 In any circumstance where an Assistant Director is unable to approve a disclosure before it is made, the staff member must notify them as soon as

[17] 1993 Act section15(1)(B)
[18] An Operations Manager is any member of staff at grade 3 or above who manages a team within the casework operations directorate.

possible afterwards. They should record their discussion with the Assistant Director and relevant information about the disclosure on Dynamics 365.

3.42 If an immediate disclosure is approved, then we must inform the subject of the disclosure we have made it as soon as practically possible to meet our legal obligations. **(Legal requirement)** The Director of Operations and Quality should also be informed that a disclosure has been made.

Compliance

3.43 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.

4 Disclosing information where there is a risk to the health and safety of a complainant or others

Introduction

4.1 This guidance explains what to do if you receive information that indicates there may be a risk (that is the probability of harm being caused) to a complainant or others (this includes children or vulnerable adults) and the situation may require us to disclose that information. The legal background contained in this policy is available in annex F and a process flow chart in annex G.

4.1 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. For example, 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.

4.2 Section 14 (2I) allows us to share decision letters or investigation reports in health cases with any person we consider appropriate[19]. We would not generally use these powers to disclose information about risk. This is because we are unlikely to share whole decision letters or reports for the purposes of alerting others to risk. The specific type of information we want to release is also unlikely to be included in these documents.

4.3 We can disclose information under section 15 of the Health Service Commissioner's Act when it relates to a likely threat to the health and safety of a patient[20]. Section 15(1)(e) only deals with situations in which we have obtained information in the course of, or for the purposes of, a health investigation[21], and that information constitutes a threat to health and safety of patients. When we make disclosures this way, we are doing so lawfully and therefore should consider whether information can be shared using section 15.[22]

4.4 There is no equivalent provision in the Parliamentary Commissioners Act 1967 that allows us to disclose information lawfully. This policy should therefore be

[19] 1993 Act, section 14 (2I).

[20] 1993 Act, section 15 (1)(e)

[21] Note: This is not restricted to investigations only and may include information obtained in intake, assessment or review stage.

[22] The guidance for making these decisions is available in section 3 of this document.

used if we want to share information with others that is obtained for the purposes of a parliamentary investigation. **(Policy requirement)**

4.5 If a staff member is unsure under which policy to disclose information then they should discuss this further with a manager and the Legal Team before taking any action. In circumstances where a disclosure needs to be made urgently and a manager or the Legal Team is not available, the staff member can still make a disclosure. They must discuss the case with a manager as soon as possible though following the disclosure being made. **(Policy requirement)**

4.6 Any action taken under this policy should be fully recorded on Dynamics 365 for our audit trail. **(Policy requirement)** The Dynamics 365 entry should include the exact information we were 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.

4.7 This policy does not cover the management of threats made to staff members. This is covered in the unreasonable behaviour policy[23].

Identifying risks

4.8 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. **(Policy requirement)** Some of the key points to think about[24] are:

- Is there a realistic risk to the individual or others? (It is not necessary to prove that the risk 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 risk.)

- Does the individual 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.

[23] The unreasonable behaviour policy is in section 2 of this document.

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

- 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?

Telephone calls

4.9 All threats of harm must be taken seriously. If in conversation with a complainant or other person they suggest there is a risk they will self-harm, attempt suicide or endanger someone else, they should, if appropriate, first be encouraged to contact the emergency services or another suitable type of assistance themselves. **(Policy requirement)**

4.10 If the complainant is able to confirm in a calm and rational way that they will follow the agreed steps and maintain their own safety, then we may decide we do not need to take any further action. The staff member taking the call must ensure they record details of the call, including the plan agreed to ensure the complainant's safety.
(Policy requirement)

4.11 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 are so concerned that we decide to act without the caller's agreement.[25]

4.12 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.[26]

4.13 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.

[25] DPA 2018 Schedule 10, Condition 3 (a), (b)/General Data Protection Regulation permits this.
[26] DPA 2018 Schedule 10, Condition 3 (a), (b)/ General Data Protection Regulation permits the sharing of sensitive personal data without consent.

Process: making a disclosure following a reactive assessment of risk

4.14 This process should be followed 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 makes a credible threat against the doctor they are complaining about.

4.15 The staff member responsible should record all stages (including analysis, discussions, decisions and any disclosure) as fully as possible (on Dynamics 365 if case related), however, this can be completed after the event. **(Policy requirement)**

- The staff member should discuss the case with a manager as soon as possible to assess the credibility of the threat and whether a disclosure may be appropriate. They do not have to seek legal or clinical advice to agree a disclosure, but if it is needed, it should be sought at this stage. Any threats to our staff, property or information must be reported to the Security Officer. **(Policy requirements)**

- If it is decided that a disclosure should be made, then details of the case should be escalated via line management to an Assistant Director or above for approval in line with the Delegation Scheme. If an Assistant Director cannot be contacted quickly, then an Operations Manager (or a manager of a higher grade) or a Senior Solicitor can, exceptionally, approve the disclosure. **(Policy requirement)**

- This approval should be clearly recorded on Dynamics 365. We can make a disclosure after a verbal authorisation. This must be confirmed later though, for example, by email or by a note on the case record. **(Policy requirement)**

- The approval decision must include agreeing the organisation(s) to which we are disclosing the information to. In the most urgent cases, the disclosure is likely to be to the emergency services. In appropriate cases we may additionally consider contacting other people or services, such as a mental health crisis team, social/support worker or GP. If the threat comes from an individual with a diagnosed 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 unlikely that a staff member 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, Operations Manager or a Senior Solicitor cannot be contacted immediately, a staff member may make the disclosure without prior authorisation. In these circumstances, the staff member should notify an Assistant Director as soon as possible

afterwards and record relevant information about the disclosure on Dynamics 365. **(Policy requirement)**

- A staff member who is working from home, or is a member of our associate team, should attempt to get approval before making a disclosure. There will be instances though when they may have to make a disclosure without prior authorisation. For example if a complainant is on the telephone and threatens self-harm, and the staff member cannot get in contact another way. **(Policy requirement)**

- The staff member should consider telling the subject of the disclosure that we are proposing to share information about them with a third party **before** doing so. There will be occasions when this will not be appropriate, for example, a complainant tells us if we speak to their GP about their suicidal thoughts then they will self-harm.

- We should ensure we disclose the minimum amount of factual information needed to mitigate the risk to the minimum number of organisations. This includes not providing information about any case we are considering or investigating, unless absolutely necessary in order to explain why we are making the disclosure. **(Policy requirement)**

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

- When the staff member speaks to the person they are disclosing information to, they should tell them they are giving confidential information for the sole purpose of mitigating the risk in question. If possible/appropriate, they 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 subject of the disclosure that the information that initiated its action came from us.

  (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 staff member concerned may need to stay in the office beyond their usual office hours. If they are unable to remain at work to complete an urgent disclosure, the manager should make the disclosure on their behalf or ensure that another staff member has all the information necessary to do so. Managers should, as far as is possible, make sure that no one is left in the office by themselves while making the disclosure.

After making the disclosure

- If not already completed, the staff member should ensure each stage of the process and the relevant approvals have been recorded on Dynamics 365. This should include explaining the reasons why the disclosure was required and cross-referencing to relevant evidence and advice (including clinical). **(Policy requirement)**

- If the disclosure relates to a specific case, the staff member should review the risk rating on Dynamics 365 and ensure that any mitigation plan is up to date. (Further information about assessing the risk rating in cases is available in section 1 of the general guidance. Whether the risk rating needs to be changed will depend on the individual circumstances of the case, however both the risk rating and any mitigation plan should be regularly reviewed. **(Policy requirement)**

- If not already completed, we should inform the person involved that we have made a disclosure and who we have made it to. If applicable, we should also inform any person who provided us with the information that we have shared it. **(Policy requirements)**

Process: making a disclosure following a proactive assessment of risk

4.16 This process should be followed when we take a view that we need to disclose information because we consider our actions (or casework decisions) may lead to a risk to the health and safety of a complainant or others. This is likely to be linked to the content or outcome of a decision, provisional views or in our final investigation report , 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 a decision to a vulnerable complainant explaining we will not take further action on their case or if a complainant has threatened self-harm if we do not uphold our investigation into their complaint.

4.17 The staff member should record all stages (including analysis, discussions, decisions and any disclosure) as fully as possible on Dynamics 365.

- The staff member should discuss the case with a manager as soon as possible to decide whether a disclosure may be appropriate. This will include considering how credible the threat is. We do not have to seek legal or clinical advice, but if it is needed, it should be sought at this stage. They should also inform the Security Officer of any threats to our staff, property or information. **(Policy requirement)**

- The relevant staff member (usually the case owner) should review the case risk rating on Dynamics 365 and ensure that any mitigation plan is up to date. Whether the risk rating needs to be changed will depend on the

individual circumstances of the case, however both the risk rating and any mitigation plan should be regularly reviewed[27]. **(Policy requirement)**

- If we are to go ahead with the proposed disclosure, an Assistant Director (or above) should be contacted to approve the disclosure in line with the Delegation Scheme. If an Assistant Director cannot be contacted quickly, then an Operations Manager or a Senior Solicitor can, exceptionally, approve the disclosure. **(Policy requirement)**

- This approval should be clearly recorded on Dynamics 365. We can make a disclosure after a verbal authorisation. This must be confirmed later though, for example, by email or by a note on the case record. **(Policy requirement)**

- This approval must include agreeing the organisation(s) to which we are disclosing the information to. 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. If the threat comes from an individual with a diagnosed mental health history, our normal approach should be to disclose information to their clinician (disclosure to other parties should be considered as appropriate).**(Policy requirement)**

- The staff member should consider telling the subject of the disclosure that we are proposing to share information about them with a third party **before** doing so. There will be instances though when this is not appropriate, for example, a complainant tells us if we decide not to investigate their case they will harm themselves.

- We should disclose the minimum amount of factual information needed to mitigate the risk to the minimum number of organisations. This includes not providing information about any case we are considering or investigating, unless absolutely necessary in order to explain why we are making the disclosure. **(Policy requirement)**

- We can make the disclosure by telephone or in writing. If we use email, we should take steps to ensure that the person we are disclosing information to 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, ensuring that documents are sent securely through Egress[28]).

- The staff member making the disclosure should tell the person we are disclosing information to that we are giving confidential information for the sole purpose of mitigating the risk in question. If possible/appropriate, we should:

[27] Further information on assessing risk in casework is available in section one of this document.
[28] Further information is available at the following link: How to send a secure email in outlook using Egress

- ask the person we are disclosing information to, 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 staff member, 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. **(Policy requirement)**

- If the case also contains a Duty of Candour issue, we should contact the CQC's Safety Escalation Team at their National Customer Service Centre on 0300 0616161 to inform them of the Duty of Candour issue.

After making the disclosure

- If not already completed, the staff member should ensure each stage of the process and the relevant approvals have been recorded on Dynamics 365. This should include explaining the reasons why the disclosure was required and cross-referencing to relevant evidence and advice (including clinical). **(Policy requirement)**

- If the disclosure relates to a specific case, then the staff member should review the case risk rating on Dynamics 365 and ensure that the mitigation plan is up to date. Whether the risk rating needs to be changed will depend on the individual circumstances of the case, however both the risk rating and mitigation plans should be regularly reviewed. **(Policy requirement)**

- If not already completed, we should inform the person involved that we have made a disclosure and who we have made it to. If applicable, we should also then inform the person who provided us with the information that we have shared it. **(Policy requirement)**

Support for staff

4.18 As soon as possible after the disclosure, the manager of the staff member (the person who received the information and/or made the disclosure) should meet with them to discuss the incident, talk through their feelings and to raise any concerns or anxieties. 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. **(Policy requirement)**

4.19 The staff member and manager 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 contact [redacted]. The manager should also agree an action plan for how staff should deal with further contact with the complainant concerned (For example; reconsidering the risk rating on the case, or having correspondence go through a specific staff member). **(Policy requirement)**

4.20 We will fully support staff members 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.

5. Sharing information under the emerging concerns protocol

Introduction

5.1 The emerging concerns protocol (the protocol) was developed under the governance of the Health and Social Care Regulators Forum in October 2016.

5.2 The purpose of the protocol is to develop an approach for those organisations signed up to it[29] to share information and intelligence that may indicate risks to the users of health services (including their carers or families/professionals) in a timely fashion.

5.3 The intention of the protocol is to provide a way of sharing information that has come about as a result of investigative or regulatory action that would not normally be disclosed to other organisations. This includes allowing organisations the opportunity to be more flexible and open to sharing information more readily and earlier on in the process.

5.4 This policy provides a general overview of the protocol and explains how we should put it into practice in our organisation. The protocol document provides more detailed information about how and when concerns should be shared, and the types of information organisations may be interested in receiving.

5.5 Sharing information under the protocol is a two-way process, and we may be asked to provide it by organisations, as well as wish to share information ourselves. There are no limits within the protocol to the types of information we can share and this should be considered on a case by case basis.

5.6 Due to our position at the end of the complaints procedure, we would anticipate most of the issues raised with us via the protocol will be identified before they reach us. We recognise the importance though of supporting other organisations to ensure patients and families are protected from harm that happens when things are allowed to repeatedly go wrong.

5.7 There are no specific types of information we may share through to the protocol.

Our legislation

5.8 The laws[30] that govern our work explain that we must conduct our casework in private. They also make provisions though for us to share information in

[29] Parliamentary and Health Service Ombudsman, Care Quality Commission, General Medical Council, General Dental Council, General Pharmaceutical Council, Health and Care professions Council, Local Government and Social Care Ombudsman, Health Education England and the Nursing and Midwifery Council.
[30] The Parliamentary Commissioner Act 1967 and the Health Service Commissioners Act 1993 (as amended)

particular circumstances, for example, where there is a risk to the health and safety of patients.

5.9 When disclosing information under this protocol, we are using Schedule 1, part 2, paragraphs 11 and 12 of the DPA. This allows us to share information if it is of substantial public interest. This is included in full at Annex I.

Sharing information about an individual

5.10 The information we share under the protocol will usually relate to systemic failings across an organisation, or healthcare profession, rather than the action of an individual, or a one off incident. We should therefore consider disclosing information about individuals under our section 15 (e) policy[31], instead. For example, if we become so concerned about a nurse's conduct in a particular case that we believe a disclosure to the NMC is necessary.

5.11 If we decide we do want to share information about individuals under the protocol, then we must process this data subject to the requirements of the General Data Protection Regulation. Any concerns about doing so should be discussed with the information rights team.

When should the protocol be used?

5.12 The protocol may be used when we become aware of a situation that may not be seen as an emergency, but which may indicate a future risk. For example, we receive several complaints about hygiene within operating theatres at a Trust. We therefore identify a potential emerging concern, and share information under the protocol.

5.13 Another example could be where we repeatedly see an organisation providing poorly kept records, or where documentation is missing, and this is preventing us from being able to consider a case properly.

5.14 It may also be used when we identify a cultural issue within a health and social care setting that may be noticed, but would not necessarily be raised through alternative formal systems. For example, if we learn that nurses within a particular hospital ward are being made to feel by the organisation that they are at risk of losing their job or suffering detriment if they acknowledge a mistake.

What information we may share

5.15 There are no limits within the protocol to the types of information we can share and this should be considered and agreed on a case by case basis. This could come directly from our casework, or from research and insight we have collected about organisations within our jurisdiction. For example, through our liaison work or through trends we discover through collecting insight.

[31]Please see section 3 of the general guidance for further information

5.16 We should try to avoid disclosing information though where an individual is identifiable whenever possible. This includes not naming individuals who are linked to events triggered by the protocol or those who have provided us with the information themselves unless necessary.

5.17 We must not share information that is legally privileged. If there is any concern that the information we wish to share may be privileged we should discuss this with the information assurance, or legal teams.

Process: making a disclosure of information through the protocol

5.18 If a caseworker considers a disclosure may be appropriate, they should first discuss the case with their manager. This discussion should consider;

- Whether the issue is best handled under the protocol;
- What would need to be shared, and with what organisations;
- The credibility of the source and documentation, and;
- Whether this information could be amended to make any individuals referenced within it unidentifiable.

5.19 If it is considered a disclosure should be made, details of the case, and the proposed disclosure should be sent to the Assistant Director of Strategy and Partnerships for approval, copying in the appropriate Assistant Director from Operations and the Information Rights team.

5.20 The Assistant Director of Strategy and Partnerships[32] will then collaborate with Operations and Information Assurance to decide whether it is appropriate to share the information under the protocol, and the appropriate organisation(s) it should be shared with. This may include using the grading tool. Further information is available in the emerging concerns protocol itself.

5.21 Following consultation with others, if the Assistant Director of Strategy and Partnerships is happy for the disclosure to be made, they should record their decision on the relevant case record. The disclosure can then be made to the appropriate organisation(s).

5.22 If at any point in the process there are concerns relating to the appropriateness of sharing of information, or the format in which this should be shared, advice should be sought from the Information Rights team.

Process: receiving a request for information through the protocol

5.23 We will on occasion be asked to provide information through to the protocol to other organisations. These requests should be sent by the organisation directly to the Information Rights team.

[32] The Assistant Director of Strategy and Partnerships is currently the designated lead for the Protocol at PHSO.

5.24 When an organisation asks us to disclose information under the protocol it should be treated as an information request, and handled as such. Once the Information Rights team receive the request they should log and review it, and collate the relevant data needed to fulfil it.

5.25 Once the request is ready for sharing, it should be sent through to the Assistant Director of Strategy and Partnerships for review. If they consider the information should not be sent, they should inform the organisation of the reasons why.

5.26 If the Assistant Director of Strategy and Partnerships considers the disclosure should be made, this can be sent through to the Chief Executive for approval. If approved, the request should be passed back to the information rights team, and the information released.

5.27 If not approved, the request should be sent back to the Assistant Director of Strategy and Partnerships to inform the organisation the information will not be shared and the reasons why.

5.28 The process documented above should be fully audited on the request for information from the organisation.

Regulatory Review Panels

5.29 Regulatory Review Panels (RRPs) may be called during the protocol process. They provide an opportunity for key people from each organisation to hear and share information about the issue that has been raised. The intention is that these panels agree an appropriate coordinated intervention for that issue, such as regulatory action.

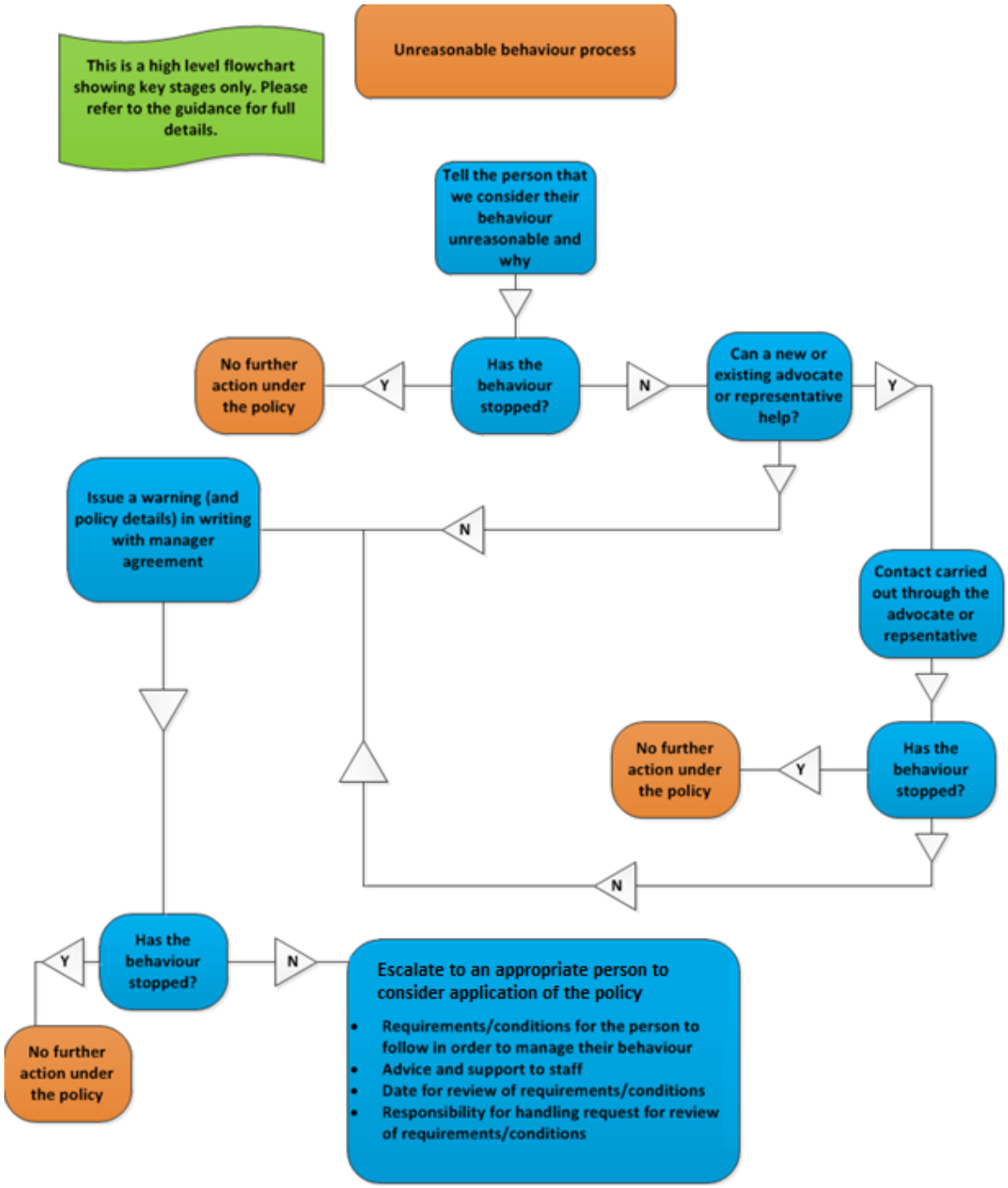
5.30 If we are invited to an RRP we will need to decide whether to attend based on the likelihood that the issue being raised may end up with us as a future complaint.

Documenting information we disclose

5.31 The Assistant Director of Strategy and Partnerships is responsible for holding a central list of when we have provided or shared information under the protocol. This will include;

- The dates for when the referral was received, and the protocol initiated;
- The details of those involved within the referral, such as the providers and professionals identified;
- Which organisations the information was shared with;
- The actions agreed and taken as a result; and
- The decisions to call or not call a RRP.

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 a copy of our 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 manager (or another manager if the manager is not available). The manager (talking to others as necessary) should 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.

Completing the form

6. The 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 Dynamics 365 case record.

9. If you need further advice please talk to your 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.

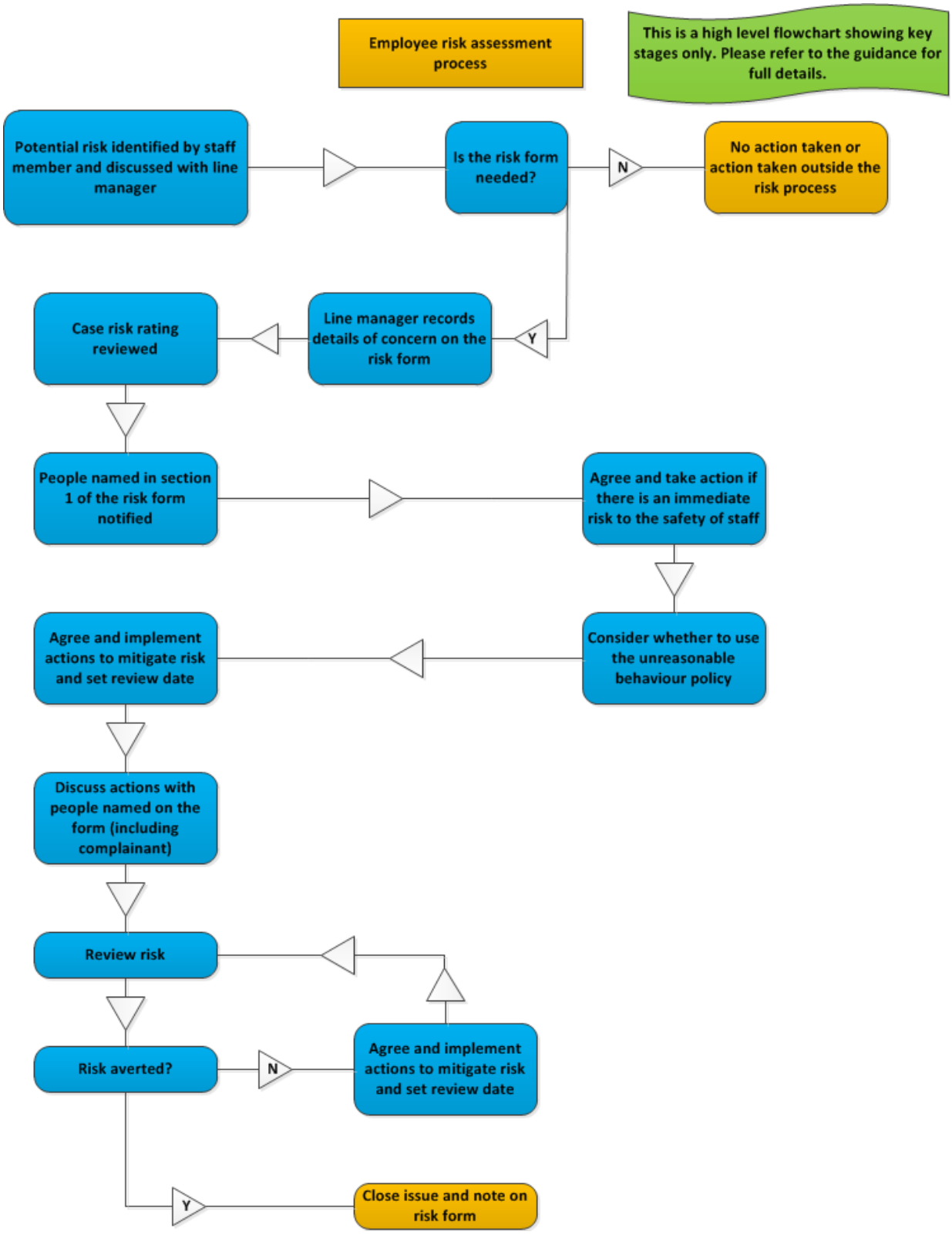
    - Section 2: A summary of the risk, how it was identified, relevant dates and any action taken so far. This must also say whether the relevant case is open or closed.

    - 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 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



Annex D: Recording information on Visualfiles

Recording a warning

1. The staff member should record the warning fully on the person's details screen on Visualfiles (this screen can be accessed by either searching for the person by name or by accessing their details from a case). **(Policy requirement)**

    - On the person'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.

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

Recording the application of the policy and restrictions

- 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.

3. Add relevant details about the restrictions imposed.

    - Select 'Add/view restrictions' (if previous restrictions are recorded then 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).

4. It is essential that the staff member dealing with the person at the time keeps Visualfiles up to date, particularly if the restrictions on contact are altered, varied or removed. **(Policy requirement)**

Recording a review of the policy

- 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 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).

Annex E: Definition of Terms

Abusive: Using language that is extremely offensive and insulting to an individual.

Defamation: A false statement made to a third party which discredits a person's character or reputation. If spoken it is slander or if published in print through some form of media, it is libel.

Offensive: Causing someone to feel upset, attacked, insulted or disrespected.

Threatening: Behaving in a hostile or deliberately frightening manner.

Harassment as defined by the Equality Act 2010: Unwanted conduct related to a protected characteristic that has the purpose of violating a person's dignity or creating an intimidating, hostile, degrading, humiliating or offensive environment for that individual.

Discrimination as defined by the Equality Act 2010: Discrimination means treating someone less favourably that someone else because of a protected characteristic. It is unlawful to discriminate someone because they have or are perceived to have a protected characteristic or are associated with someone who has a protected characteristic.

Protected characteristics: Age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion and belief, sex and sexual orientation

Annex F: 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.

Annex G: Legal background: maintaining confidentiality in our casework

- We must act in accordance with the law relating to data protection[33] 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.

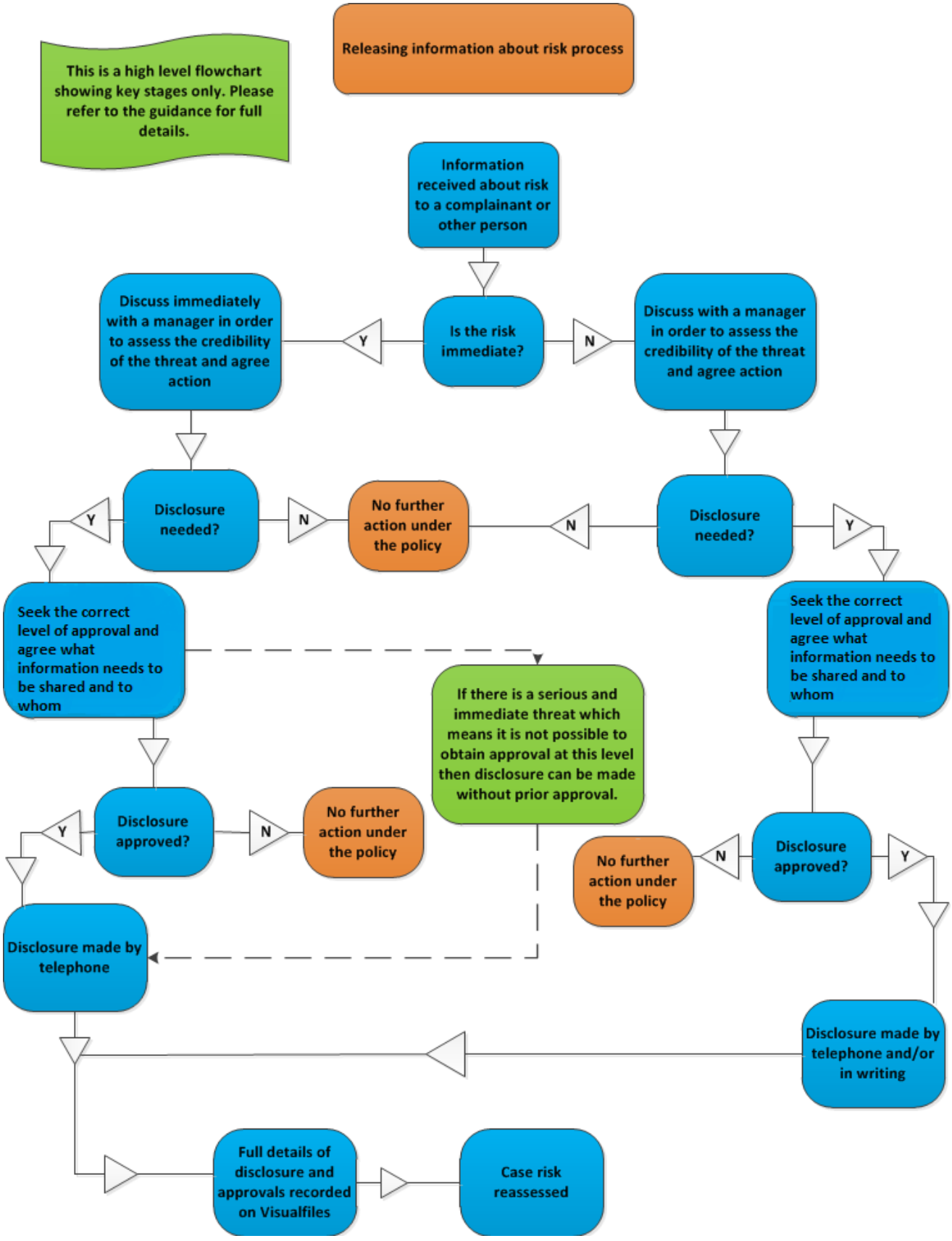
- Our legislation requires that we conduct investigations[34] in private.[35] We should make sure that we maintain confidentiality when we conduct an investigation and are aware of information that is, and is not, appropriate to share between the parties to the complaint. We may disclose information 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.[36]

- 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.[37]

- 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.

[33] *Data Protection Act 1998. Freedom of Information Act 2000.*
[34] Please note that these restrictions on the disclosure of information cover all of our casework, including assessment and review work.
[35] 1967 Act section 7(2). 1993 Act section 11(2).
[36] 1967 Act section 11. 1993 Act section 15.
[37] 1998 Act, Schedule 3, paragraph 3(a) (i)-(ii) and 3(b).

Annex H: Process flow chart



Annex I – Public interest test

Protecting the public against dishonesty etc

11(1) This condition is met if the processing—

(a) is necessary for the exercise of a protective function,

(b) must be carried out without the consent of the data subject so as not to prejudice the exercise of that function, and

(c) is necessary for reasons of substantial public interest.

(2) In this paragraph, "protective function" means a function which is intended to protect members of the public against—

(a) dishonesty, malpractice or other seriously improper conduct,

(b) unfitness or incompetence,

(c) mismanagement in the administration of a body or association, or

(d)failures in services provided by a body or association.

Regulatory requirements relating to unlawful acts and dishonesty etc

12(1)This condition is met if—

(a)the processing is necessary for the purposes of complying with, or assisting other persons to comply with, a regulatory requirement which involves a person taking steps to establish whether another person has—

(i)committed an unlawful act, or

(ii)been involved in dishonesty, malpractice or other seriously improper conduct,

(b)in the circumstances, the controller cannot reasonably be expected to obtain the consent of the data subject to the processing, and

(c)the processing is necessary for reasons of substantial public interest.

(2)In this paragraph—

- "act" includes a failure to act;
- "regulatory requirement" means—
- (a) a requirement imposed by legislation or by a person in exercise of a function conferred by legislation, or
- (b) a requirement forming part of generally accepted principles of good practice relating to a type of body or an activity.