

Business Integrity Training

Scenarios for Team Discussions 2026

Set A: IT users



Scenarios for Team Discussions pages 2-10



Further reading and support material page 12-13



Guidance for leading the scenarios pages 13-19

A message from your Executive Committee

As leaders and people managers across the organisation, we share a vital responsibility to create a positive, safe and ethical workplace. By setting clear expectations and modelling the behaviour we want to see, we can uphold the highest standards of business conduct across our organisation.

We encourage everyone to speak up if something doesn't feel right and we're committed to supporting those who do. Building a culture of openness and accountability is essential to our collective and continued success.

This year, our Business Integrity Training focuses on two key themes:

When help becomes a threat (for IT users) and **Think before you post** (for non-IT users): Exploring responsible online behaviour, the use of digital tools and the importance of safeguarding information.

Crossing the line: Addressing sexual harassment and reinforcing the importance of ensuring everyone feels safe, respected and protected at work.



A message from your Executive Committee

Why these topics matter

Protecting information: The first scenario highlights the critical role we play in safeguarding valuable information and using online tools responsibly. We're all trusted – by the company, our customers and our colleagues – to get this right and mismanaging information or the use of online tools can have serious consequences. Please use this scenario to ensure your team understands our guidance and knows where to seek support if needed.

Protecting our people: The second scenario explores sexual harassment and emphasises the importance of ensuring everyone feels physically and psychologically safe, respected and supported at work. Please let your teams know that we are extremely grateful to every colleague who has spoken up about unacceptable behaviours because they're not only protecting themselves – they're protecting their colleagues too, and holding us all accountable to our Code of Conduct.

We understand that discussion of this topic may be difficult for colleagues who have personally experienced sexual harassment or other inappropriate behaviours, and you are empowered to offer alternative ways to experience this training if you believe a group discussion would be challenging to your or a colleague's wellbeing.

Speaking up: We recognise that raising concerns can be difficult, but it's always the right thing to do. Please reassure your teams that as leaders and managers we are all here to listen, take action and provide support. Remind them of the many avenues available for raising concerns, including you, as their manager, the HR function, our Ethics Officers or our Ethics Helpline which can be anonymous.
Thank you for the incredible and important work you do to support your team(s) and help us fulfil our mission to protect those who protect us – and each other.



Set A (IT users): Scenario 1

When help becomes a threat

Two months into a new position, Marcus was keen to impress in this new role and was working hard on a critical project. Whilst striving to meet a deadline, he made use of publicly available online tools to help him with his workload, that are not approved by the Company. The information entered into the online tools contained colleagues' personal information, controlled technical specifications and sensitive company information. Marcus briefly considered whether it was appropriate to enter the information into the online tools but concluded that "it must be fine", because he could access them from his work laptop.

At the weekend, Marcus updated his LinkedIn profile on his personal device, keen to update his job description and share the experience it has provided to him. In his profile update, Marcus included his security clearance and highlighted the project he was working on, referencing its name, listing some of the technology being developed and described some of the technical specifications.



Marcus is pleased with the outcome of the work he has produced by using the online tools and shares what he did with his colleagues during the next team check in.



Set A (IT users): Scenario 1

Questions for Discussions

1. What concerns do you have about Marcus's actions?
2. If using publicly available internet tools for work purposes, what should you consider to keep the Company's information and its customers', partners' and employee's information safe?
3. What do you think about Marcus sharing project information and his security clearance on social media?
4. To further explore the theme of ensuring Company information and assets remain secure, what should happen when someone moves roles or leaves the Company?



Set A (IT users): Scenario 1

Continue after the discussion questions on the previous page

Concerned about the details of the information that Marcus has input into the online tools, one of Marcus's colleagues raised their concern to their line manager.

The next day, Marcus was called into a meeting with his line manager along with a HR representative. They explained that all the information that Marcus entered into the online tools and his LinkedIn profile is now stored on servers outside the Company's control, in unknown locations where it may be widely accessible. The incident triggered multiple compliance concerns:

- **security** policy violations that exposed confidential Company information and potentially undermines national security;
- possible breaches of **export control** regulations through the transfer of controlled information to unauthorised third parties; and
- potential breach of **data protection** law due to potential unauthorised disclosure and processing of personal data.

In addition, **in the defence industry, oversharing on social media can pose significant business and personal security risks**, as it can expose sensitive information that adversaries or malicious actors might exploit.

Outcome:

These issues could in result in reputational damage to the Company and undermine the trust of customers and regulators. As a consequence of Marcus's actions, an internal investigation will need to be initiated to access the implications of the data loss and to identify any potential violations of export control and data protection laws.

Marcus is likely to face disciplinary action for breaching Company policies, which could result in a formal sanction, up to and including dismissal for gross misconduct. In addition, regulatory violations may result in fines or criminal proceedings against Marcus and the Company.



Set A (IT users): Scenario 1

Key Messages

Security

- Our Security Policy requires us all to safeguard assets (including information) from loss, damage or compromise. We are required to manage all assets in accordance with their classification and relevant handling instructions.
- Online tools include web-based services like Generative AI, file-sharing platform and translation services and bots used to transcribe meetings. These tools present a risk to our Company and customers by potentially spreading malicious software through downloads and compromising information security, as we don't know where it is stored or processed, or who has access to the information once it is entered.
- Any unapproved online tools must not be used for any information that is not intended to be publicly available.
- The Company-approved tool (Enterprise Copilot) offers the best protection against these threats when used correctly (if approved for use in your business).
- Follow Company-issued guidance on using all Generative AI tools and other online tools, including Enterprise Copilot.

Use of Social Media

- Follow the BAE Systems Social and Digital Media Guidelines, in particular, employees should not share any confidential Company information or their security clearance, if applicable, on any form of social media or digital media.
- Sharing information about the work you are involved in at BAE Systems could make you a target to hostile actors looking to gather information or harm the Company.
- Refer to the Group Security Intranet pages and the Spark Security Academy for best-practice security advice and further help.

Export control

- Be familiar with the Company's policies and procedures for handling export-controlled items and/or providing services.

- Understand the rules for accessing, sharing, sending and receiving export-controlled material, even if it is not a day-to-day part of your role.

Personal information

- Ensure that any personal information you collect, use, or have access to as part of your role is handled appropriately. Follow Company policies, processes and procedures for handling personal data. Only use Company-approved resources and processes so that you can be sure that appropriate controls are in place to reduce the risks of loss, alteration and unauthorised disclosure of, or access to, personal data.
- If unsure contact your local Data Protection lead to confirm any governance steps required when handling personal information. A list of local Data Protection leads can be found at: Global Intranet > Functions (tab) > Legal > Personal Data Protection.

Responsible behaviour

- We should all take responsibility for doing the right thing and engage only in actions that are ethical and legal in accordance with standards and expectations of our Company Code of Conduct.
- If you have any concerns, speak up and report them promptly, which you can do anonymously if preferred. This helps to protect our Company, our employees and our stakeholders.

Disciplinary sanctions

- An appropriate disciplinary sanction shall depend on the particular facts of each case, including, but not limited to, severity of misconduct, the individual's intentions and context in which the conduct occurred and an individual's disciplinary record and any mitigating circumstances.



Set A (IT users): Scenario 2

Crossing the line?

Content Warning: The discussion for this scenario focuses on the topic of **sexual harassment**, which some participants may find distressing. Please take care of yourself and your team around this content and seek support as needed.

Jamie, a recent graduate, has been working closely with Tam, an experienced senior manager who has worked at the Company for a long time. Tam is leading a project that Jamie is working on.

What began as professional guidance quickly evolved into a close working relationship, with Jamie feeling grateful for Tam's career advice and personal interest in their development.

Tam began offering increasingly personal support, suggesting one-on-one dinners outside of work to "discuss career goals" and giving thoughtful gifts to celebrate Jamie's professional milestones.

Their conversations shifted from career development to more personal matters.



As months passed, Tam began making comments about Jamie's appearance and following Jamie's social media with late night personal messages.

At the team's end-of-year celebration, after several drinks, Tam cornered Jamie, placed a hand on Jamie's lower back and suggested they leave together.

Several colleagues noticed Tam's behaviour towards Jamie but hesitated to speak up, thinking it wasn't their place to interfere. One colleague considered reporting it, but worried about challenging a senior manager and did not want to get involved.

Set A (IT users): Scenario 2

Questions for Discussions

1. Do you think Tam's behaviour crossed professional boundaries and, if so, at what point?
2. How would you describe Tam's behaviour? Do you think Tam's behaviour is sexual harassment and why?
3. Why is it necessary to intervene when you witness inappropriate behaviour, even if you're not directly involved?
4. What are the qualities of a positive mentoring experience?
5. What responsibilities do individuals have when drinking at work functions?



Set A (IT users): Scenario 2

Continue after the discussion questions on the previous page

Jamie felt increasingly uncomfortable about Tam's advances, but didn't want to appear ungrateful for the interest Tam had taken in Jamie's professional development.

Jamie feared that rejecting Tam's unwelcome attention could create tension and have career consequences, especially because of Tam's seniority.

Jamie shared their concerns with Ethics after receiving assurance about the Company's position on retaliation. Ethics passed the matter to the relevant HR team for investigation. Safeguards were implemented for both parties during a disciplinary investigation and disciplinary process.

During this time, Jamie and Tam were provided with support and regular wellbeing check-ins by their line managers and Ethics.



Outcome:

An independent manager was appointed to ensure an impartial investigation. Jamie, Tam and several witnesses provided statements. Tam denied the actions were sexual, stating that Jamie had misconstrued friendliness and Tam's tactile nature.

During the investigation, Jamie provided copies of text messages from Tam containing sexually explicit content.

Disciplinary proceedings commenced. The Disciplinary Manager concluded that Tam's behaviour constituted sexual harassment: it was unwelcome and sexual in nature and created a hostile environment for Jamie. The behaviour was considered particularly serious due to its persistence and Tam had exploited the power imbalance between them.

Tam was dismissed from the Company with immediate effect for gross misconduct.



Set A (IT users): Scenario 2

Key Messages

Unacceptable Behaviours: Sexual Harassment

- We should treat each other with courtesy, dignity and respect.
- Harassment through any means, including verbal, non-verbal, physical or online will not be tolerated. Abusive, offensive, humiliating or intimidating behaviour is never acceptable.
- Harassment can occur in many different configurations, regardless of age, gender, or position with the Company. For example, a younger employee harassing an older one, same-gender harassment, or harassment by a subordinate or a more senior colleague.

Psychological Safety and Speaking up

- An inclusive culture is one where everyone is respected, valued and able to contribute. Psychological safety is essential to this, ensuring employees feel confident to speak up and raise concerns without fear of embarrassment, negative consequences, or retaliation. It also enables innovation, higher engagement, empowerment and trust, which are essential for business performance and growth.
- Speaking up is the act of voicing a concern; the Company encourages all employees to speak up if they see anything that they think isn't right, whether this directly affects you or whether you are a witness.
- Speaking up is a vital aspect of maintaining a culture of integrity and ethical behaviour.
- Everyone should feel able to speak up, knowing they will be treated with respect. Often an issue can be resolved by speaking with the person concerned, or alternatively you can report your concerns to your line manager, HR or reach out to Ethics.
- Delaying action until behaviour escalates places those experiencing inappropriate conduct at greater risk and allows harmful patterns to take root. Raising concerns early,

when boundaries first begin to blur, can prevent more serious harm.

- Psychological safety is created by normalising open and respectful conversations about uncomfortable interactions before they become severe.
- The Company strongly encourages all employees to speak up. Retaliation against anyone who raises a concern in good faith will not be tolerated. All reports of unacceptable behaviour are taken seriously and will be assessed and investigated.
- Contact methods and the Speak Up Guide can be found by going to the global intranet and following: **Employees > Ethics Helpline**. Further information can also be found in the Dignity and Respect Standards.

Responsible Mentoring Relationships

- Mentoring must follow company guidance and be recorded on relevant learning systems.
- Mentors and mentees should behave professionally and in accordance with the Code of Conduct and the Dignity & Respect Standards at all times, maintaining clear professional boundaries.
- The Mentoring at BAE Systems Guide is linked on page 11.

Disciplinary sanctions

- An appropriate disciplinary sanction shall depend on the particular facts of each case, including, but not limited to, severity of misconduct, the individual's intentions and context in which the conduct occurred and an individual's disciplinary record and any mitigating circumstances.



Further reading & Support material



Code of conduct

- Speak Up diagram (page 12)
- Respect at work (page 18)
- Using Company IT systems (page 32)
- Managing, handling and sharing information (page 34)
- Personal information (page 36)
- Export controls, sanctions and restrictions (pages 70)

Our Code of Conduct can be found on the global intranet under **How we work > Code of Conduct**

Policies

- Export Control Policy
- Security Policy
- Personal Data Protection
- IT Acceptable Use Policy
- People Policy
- Operational Framework: Our Values

Group policies can be found on the global intranet under **How we work > Operational Framework > Policies, Processes and Charters**.

Guidelines

- [Guidance of the use of Generative AI](#)
- [Social and Digital Media Guidelines](#)
- [Mentoring At BAE Systems Guide](#)

Additional sources of support:

- [ConnectHub Artificial Intelligence Hub](#)
- [Ethics Helpline](#)
- [Speak Up Guide](#)
- Responsible Decision-Making Model (see page 13)
- [Mental Health and Wellbeing intranet page](#)
- [Dignity and Respect Standards \(UK only\)](#)
- [Employee Assistance Programme \(UK only\)](#)
- [Safeguarding Teams for Apprentices \(UK only\)](#)

Our Code of Conduct cannot cover every situation that we may find ourselves in. **Our Values**, along with the **Responsible Decision-Making Model**, can help guide us through.

Further reading & Support material

Helping you navigate tough decisions

Use our decision-making model to guide you to the right decision.

1. Gather the facts

Do I have all the relevant information?



2. Understand the rules

What are the relevant laws and regulations?



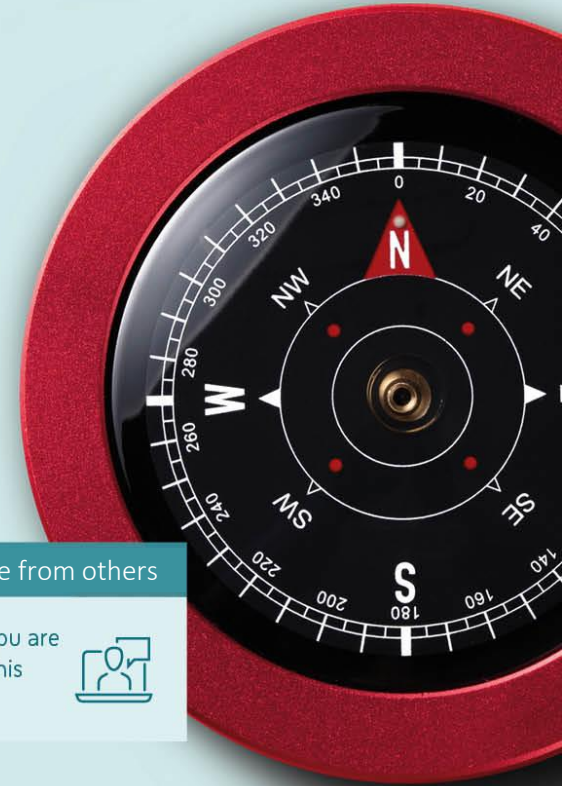
3. Consider the situation

Think about our principles of accountability, honesty, integrity, openness and respect.



4. Seek advice from others

Remember you are not alone in this process.



Our Code of Conduct.
Your guide to doing the right thing.

BAE SYSTEMS



Guidance for Leading the Scenarios

Who should do the training? The Scenarios for team discussions 2026 are **mandated for all of BAE Systems Plc managed business** (excluding Inc.) that are on the headcount report up to 31st December 2025. **Contingent Labour are expected to undertake this training and to comply with its provisions.** New starters from 1st January 2026 are encouraged to do the training with your team and can be recorded via the retro upload form.

Why are we doing this training? As a Company, we want our employees to **engage in regular, live training, to foster discussion about business conduct.** The Executive Committee mandates that these discussions take place each year, which should be management-led engagements.

Long-term absence/maternity/paternity? If you have a member of your team on long-term absence for the rest of 2026, please advise bitsupport@baesystems.com of this including their name, GCI, email address and reason for them receiving a waiver for this year's training. If the absence is planned, you should deliver the training where possible before they go on leave.

How do I record that the learning has taken place? Once your team has completed the training record completion using the retro-upload form [available here](#) and send it to bitsupport@baesystems.com. Facilitating a session can count as completion of training.

The BIT Support team need the retro-upload form to be sent in its original format, as an excel spreadsheet, to record the completion. Please do not save the form as any other file type.

More information can be found on the BIT Intranet page: [Global intranet > How we work > Business Integrity Training > BIT Scenarios for Team Discussions 2026](#)



Guidance for Leading the Scenarios

Your role is to facilitate a discussion guided by those questions and to demonstrate that you are a leader who welcomes diversity of thought and opinion.

Before the session

1. Prepare

- ☐ Make sure you have the correct pack most relevant to your team. There are two sets available: Set A for **IT users** and Set B for **non-IT users**. Both scenarios from the chosen set must be completed in the discussion..
- ☐ Schedule at least **30 minutes** in a standalone or existing team meeting for the session. For large teams, consider breaking into smaller groups or running more than one session.
- ☐ Make your team aware of the **scenario themes** beforehand to best prepare them for the session.
- ☐ Prepare a **list of team members** to check them off in the session. This will help when recording who has received the training.

2. Know the materials

- ☐ Read and understand the **material** you are using; it is all available in this pack. Pay particular attention to the **Questions and Key Messages** in the guidance.
- ☐ Prepare enough hard copies of the **scenarios for team discussion** (pages 2-13), if required. Only print what is necessary and use alternative ways to view the scenarios if possible.
- ☐ Familiarise yourself with the **Code of Conduct** and the **Responsible Decision-Making model**.

Delivering the session

3. Introduce the session

- ☐ For example: *"Welcome to this year's Business Integrity Training team discussions. The aim of this session is to give us an opportunity to look at situations that might occur at work and then discuss the right thing to do if they happened in our team."*
- ☐ Explain to your team why we are doing this training.
- ☐ Reference the EC's message about its importance.
- ☐ Outline the themes of the scenarios you will discuss. The scenarios are drawn from real reported incidents.

4. Share the scenarios

- ☐ **Engage your team** in reading through the scenarios for team discussion. Use pages 2-13 in this pack.

Useful tips in leading the discussion:

- ☐ Use the **Questions section** to guide the discussion.
- ☐ Think about how to make the session **engaging** and **valuable**: have the themes been in the newspapers recently?
- ☐ Ask **open-ended questions**.
- ☐ Encourage **balanced participation** from everyone.
- ☐ Encourage participants to share **relevant personal experiences**.
- ☐ Remember, you don't need to have all the answers.
- ☐ **Share the EC video** after your team discussions.

After the session

5. Close the session

- ☐ Address any **raised questions** and confirm the process for **unanswered questions**.
- ☐ Inform your team about further reading and **support material** on page 11-12.
- ☐ Record the names of **all attendees**.
- ☐ Thank participants for sharing their views.

6. Record attendance

- ☐ Use the retro-upload form to record the attendance for the session: [link here](#)
- ☐ Send the retro-upload form to: bitsupport@baesystems.com.

7. Ongoing conversations

- ☐ Follow up on any outstanding questions.
- ☐ Continue to discuss the key messages and themes in this training throughout the year, as the need arises.
- ☐ Encourage your team to speak up with any concerns or issues they may have.



Guidance for Leading the Scenarios

Scenario 1: Key Messages

Security

- Our Security Policy requires us all to safeguard assets (including information) from loss, damage or compromise. We are required to manage all assets in accordance with their classification and relevant handling instructions.
- Online tools include web-based services like Generative AI, file-sharing platform and translation services and bots used to transcribe meetings. These tools present a risk to our Company and customers by potentially spreading malicious software through downloads and compromising information security, as we don't know where it is stored or processed, or who has access to the information once it is entered.
- Any unapproved online tools must not be used for any information that is not intended to be publicly available.
- The Company-approved tool (Enterprise Copilot) offers the best protection against these threats when used correctly (if approved for use in your business).
- Follow Company-issued guidance on using all Generative AI tools and other online tools, including Enterprise Copilot.

Use of Social Media

- Follow the BAE Systems Social and Digital Media Guidelines, in particular, employees should not share any confidential Company information or their security clearance, if applicable, on any form of social media or digital media.
- Sharing information about the work you are involved in at BAE Systems could make you a target to hostile actors looking to gather information or harm the Company.
- Refer to the Group Security Intranet pages and the Spark Security Academy for best-practice security advice and further help.

Export control

- Be familiar with the Company's policies and procedures for handling export-controlled items and/or providing services.

Summary

Marcus, new in his position, working to meet a deadline, used publicly available unauthorised tools on the internet. The information he disclosed contained personal information, controlled technical specifications and sensitive Company information. He also updated his LinkedIn profile with his security clearance and sensitive project details.

- Understand the rules for accessing, sharing, sending and receiving export-controlled material, even if it is not a day-to-day part of your role.

Personal information

- Ensure that any personal information you collect, use, or have access to as part of your role is handled appropriately. Follow Company policies, processes and procedures for handling personal data. Only use Company-approved resources and processes so that you can be sure that appropriate controls are in place to reduce the risks of loss, alteration and unauthorised disclosure of, or access to, personal data.
- If unsure contact your local Data Protection lead to confirm any governance steps required when handling personal information. A list of local Data Protection leads can be found at: Global Intranet > Functions (tab) > Legal > Personal Data Protection.

Responsible behaviour

- We should all take responsibility for doing the right thing and engage only in actions that are ethical and legal in accordance with standards and expectations of our Company Code of Conduct.
- If you have any concerns, speak up and report them promptly, which you can do anonymously if preferred. This helps to protect our Company, our employees and our stakeholders.

Disciplinary sanctions

- An appropriate disciplinary sanction shall depend on the particular facts of each case, including, but not limited to, severity of misconduct, the individual's intentions and context in which the conduct occurred and an individual's disciplinary record and any mitigating circumstances.



Guidance for Leading the Scenarios

Questions for Discussions: Scenario 1

The following questions are included in the **Scenarios for Team Discussions** content and need to be shared and discussed with your team as part of the session. Below is a summary of the questions and related answers to support you in guiding the discussion around the scenarios.



What concerns do you have about Marcus's actions?

- Rushing to make a good impression may have unintentionally exposed the company to risk.
- Security policy violations may have exposed confidential Company information and potentially undermined national security.
- Possible breaches of export control regulations through the transfer of controlled information to unauthorised third parties.
- Potential violation of data protection laws due to potential unauthorised access to personal data.
- Sharing information about the work you are involved in at BAE Systems makes you a target to hostile actors looking to gather information or harm the Company.
- Company reputation damage, financial costs of investigation, remediation and potential regulatory fines.

If using publicly available internet tools for work purposes, what should you consider to keep the Company's information and its customers', partners' and employee's information safe?

- Enterprise Copilot Chat is the Company's recommended Generative AI tool for Company information (if approved for use in your business).
- Follow Company guidance when using all Generative AI tools and other online tools, even Enterprise Copilot. Failure to do so could result in a data breach and loss of confidential information and intellectual property.
- Using any unapproved tools presents an unmanaged risk to our Company and customers that could result in the loss of sensitive data or spread malicious software through downloads. We don't know where the data is, where it is being processed, or where it ends up.

What do you think about his sharing on social media?

- Marcus overshared sensitive Company information and details of his security clearance on LinkedIn, which is a security risk.
- Keep your profile professional and security-aware.
- Social media platforms, like LinkedIn, are targets for hostile actors, as they increase risks such as phishing, impersonation, espionage and personal targeting - for both you and your colleagues.
- Follow the BAE Systems Social and Digital Media Guidelines, in particular, employees should not share any confidential Company information on social and digital media.

To further explore the theme of ensuring Company information and assets remain secure, what should happen when someone moves roles or leaves the Company?

- When someone leaves the Company, for any reason, their access to Company information and assets must end immediately upon leaving. Prompt action to formalise the leaver process is critical in preventing unauthorised access to Company information and assets, including:
 - immediate access revocation (all systems and remote access);
 - recovery of Company assets (devices, physical assets, Company data); and
 - recovery of Security identification passes.
- This is not solely a HR or IT task: managers play an active role in ensuring this is done promptly when someone leaves the Company.
- Access to Company information should also be reviewed and adjusted as someone moves roles.

Guidance for Leading the Scenarios

Scenario 2: Key Messages

Unacceptable Behaviours: Sexual Harassment

- We should treat each other with courtesy, dignity and respect.
- Harassment through any means, including verbal, non-verbal, physical or online will not be tolerated. Abusive, offensive, humiliating or intimidating behaviour is never acceptable.
- Harassment can occur in many different configurations, regardless of age, gender, or position with the Company. For example, a younger employee harassing an older one, same-gender harassment, or harassment by a subordinate or a more senior colleague.

Psychological Safety and Speaking up

- An inclusive culture is one where everyone is respected, valued and able to contribute. Psychological safety is essential to this, ensuring employees feel confident to speak up and raise concerns without fear of embarrassment, negative consequences, or retaliation. It also enables innovation, higher engagement, empowerment and trust, which are essential for business performance and growth
- Speaking up is the act of voicing a concern; the Company encourages all employees to speak up if they see anything that they think isn't right, whether this directly affects you or whether you are a witness.
- Speaking up is a vital aspect of maintaining a culture of integrity and ethical behaviour.
- Everyone should feel able to speak up, knowing they will be treated with respect. Often an issue can be resolved by speaking with the person concerned, or alternatively you can report your concerns to your line manager, HR or reach out to Ethics.
- Delaying action until behaviour escalates places those experiencing inappropriate conduct at greater risk and allows harmful patterns to take root. Raising concerns early, when boundaries first begin to blur, can prevent more serious harm.

Summary

This scenario explores the misuse of power between a graduate, Jamie and an experienced manager, Tam. It demonstrates how power dynamics, age differences and career vulnerability can create complex situations. Tam's behaviour crosses into inappropriate personal situations and colleagues are concerned but do not report it.

- Psychological safety is created by normalising open and respectful conversations about uncomfortable interactions before they become severe.
- The Company strongly encourages all employees to speak up. Retaliation against anyone who raises a concern in good faith will not be tolerated. All reports of unacceptable behaviour are taken seriously and will be assessed and investigated.
- Contact methods and the Speak Up Guide can be found by going to the global intranet and following: **Employees > Ethics Helpline**. Further information can also be found in the Dignity and Respect Standards.

Responsible Mentoring Relationships

- Mentoring must follow company guidance and be recorded on relevant learning systems.
- Mentors and mentees should behave professionally and in accordance with the Code of Conduct and the Dignity & Respect Standards at all times, maintaining clear professional boundaries.
- The Mentoring at BAE Systems Guide is linked on page 11.

Disciplinary sanctions

- An appropriate disciplinary sanction shall depend on the particular facts of each case, including, but not limited to, severity of misconduct, the individual's intentions and context in which the conduct occurred and an individual's disciplinary record and any mitigating circumstances.



Guidance for Leading the Scenarios

Questions for Discussions: Scenario 2

The following five questions are included in the **content to deliver in the scenario training** section and need to be shared and discussed with your team as part of the session. Below is a summary of the questions and related answers to support you in guiding the discussion around the scenarios.



Do you think Tam's behaviour crossed professional boundaries and, if so, at what point?

- Early warning signs: suggesting one-on-one dinners outside of work, giving thoughtful personal gifts, shifting conversations from career to personal matters and following Jamie's social media and sending late night messages.
- Clear inappropriate behaviour: making comments about Jamie's appearance, uninvited physical contact with intimate implications at the end of year celebration and possible propositioning (suggesting they leave together).



How would you describe Tam's behaviour? Do you think Tam's behaviour is sexual harassment and why?

- Sexual harassment occurs where both:
 - a person engages in unwanted conduct of a sexual nature; and
 - the conduct has the purpose or effect of either violating another person's dignity, or creating an intimidating, hostile, degrading, humiliating or offensive environment for that person.
- Determining whether behaviour is sexual harassment is not always straightforward. On the facts provided so far, the cumulative intense personal interest by Tam in Jamie could be sexual in nature and the physical contact and suggestion of leaving together may also be sexual.
- The facts provided here are limited and we do not know whether this attention is wanted or unwanted by Jamie. We don't know if it has the purpose or effect of violating Jamie's dignity or creating an intimidating, hostile, degrading, humiliating or offensive environment for Jamie.



Why is it necessary to intervene when you witness inappropriate behaviour, even if you're not directly involved?

- Bystander silence can have the consequence of enabling harmful behaviour to continue and escalate.
- Collective inaction indicates to all that the behaviour is acceptable.
- The vulnerable person may feel powerless to act, bystanders with less at stake have more freedom to intervene.
- We all have a responsibility for maintaining courtesy, dignity and respect. Early intervention can prevent escalation and more serious harm.

What are the qualities of a positive mentoring experience?

- Effective mentoring benefits the mentor, the mentee and the organisation by promoting a development culture, increasing knowledge sharing, driving performance and expanding networks.
- Refer to the Mentoring at BAE Systems guidance for more information.

What responsibilities do individuals have when drinking at work functions?

- Alcohol is never an excuse for inappropriate behaviour. Individuals must maintain professional conduct regardless of consumption. If someone knows they struggle with alcohol intake boundaries, they should limit their intake at work events.
- Being intoxicated does not remove accountability. Alcohol may lower inhibitions, but as individuals we are ultimately responsible for our choices.
- Leaders set the tone at Company events. Alcohol, if served, should be moderate, accompanied by food and non-alcoholic options and never on an unlimited basis.

Business Integrity Training

Scenarios for Team Discussions 2026



Thank you

for completing the Business Integrity Training scenarios for team discussions 2026.

We welcome your feedback about this training. Please email any thoughts or suggestions to:

bitsupport@baesystems.com

This publication is issued to provide outline information only. No advice given or statements or recommendations made shall in any circumstances constitute or be deemed to constitute a warranty or representation by BAE Systems as to the accuracy or completeness of such advice, statements or recommendations. BAE Systems shall not be liable for any loss, expense, damage or claim howsoever arising out of the advice given or not given or statements made or omitted to be made in connection with this document. No part of this document may be copied, reproduced, adapted or redistributed in any form or by any means without the express prior written consent of BAE Systems.