

HELPFUL WARNING! - STRICT TIMINGS FOR EACH SLIDE:
TOTAL inc QNS – 60 MINS

SLIDE 1

TIMING: 2 MINUTES

? QUESTION TO AUDIENCE:

What does the 'Data Protection ident/logo' mean to you?
What can you see?

Prompts:

Padlock

Railway track

Person

Gate

- Some people say it's about **security** – and that's certainly an important part – but the image on the screen shows that it's also about other things.
- You can see a **padlock**, but you can also see a **gate** – for better sharing of information – this is as much about appropriate access as it is about security.
- And central is a **person** - because we mustn't ever forget that data protection is about *people's* personal information.
- As well as the obligations we have, as Network Rail employees, to treat people's information in a fair, accountable and safe way, we also have our own rights, both inside and outside the workplace.
- Data protection isn't about having to lock everything down.
- It's about having the right information, with the right team, for the right reason.
- There are people at the centre of personal information held.

SLIDE 2

TIMING: 1 MINUTE

We have the news of the appointment of Andrew Haines OBE as our new chief executive, who will/has replace/d Mark Carne.

And the Data Protection team will continue its programme of work with him.

- As Mark Carne indicates here, **information is one of our greatest assets**.
- We can perhaps have a focus on our physical assets, and understanding them, of which there are plenty.
- But actually, information in this context, **personal information** is incredibly valuable.
- The five most profitable companies in world are all information and data companies...
- ...They are: Google, Facebook, Microsoft, Apple, Amazon.
- They are all companies that trade in data.
- Previously, the most valuable companies were in the oil and mining industries.
- Data is now the new oil, and this is the raw material that makes these companies the most profitable in the world.
- To deliver as a high-performing organisation, we must know **what** information we have, **where** we hold it, and **who** has access to it. We must handle this information in a way that is **fair, accountable** and **safe**.

SLIDE 3

TIMING: 1 MINUTE

- The General Data Protection Regulation, the GDPR, is the biggest shake up in data protection law in 20 years.
- It seeks to unify and clarify separate EU legislation...
- ...And bring it into the fast-developing technological world we live in.

? QUESTION TO AUDIENCE:

Would you like to guess when Network Rail employed its first data protection officer which responds to that legislation?

ANSWER:

2014!

- It provides greater protection for personal information, and brings data protection up-to-date with advancements in technology.
- This briefing will highlight some of the key elements of GDPR, and encourage us all to handle people's personal information in a way that's compliant with the law, and good for our business.

SLIDE 4

TIMING: 5 MINUTES, 44 SECONDS

PRESENTER INSTRUCTIONS:

PLAY FILM...

***...WHICH YOU SHOULD HAVE DOWNLOADED IN ADVANCE FROM
THE CASCADE BRIEFING PACK***

Play the 'Breaches' film – length - 5 minutes, 44 seconds

The film features Jeremy Bullock, programme manager, GDPR Readiness Programme

SLIDE 5

TIMING: 2 MINUTES

? QUESTION TO AUDIENCE:

So, what is personal information?

AFTER AUDIENCE RESPONSE – PRESS ‘NEXT SLIDE’ FOR THE ANSWER

ANSWER:

- Personal information (also called personal data) is any information relating to someone you can or could identify.
- Personal information is any information relating to an identified, or identifiable, individual.

The law has changed and to be compliant with the new requirements Network Rail needs to:

- Show that we think about people’s privacy in everything we do.
- Make sure that we’re open and clear with people about our use of their personal information.
- Identify and manage data protection risk, where it looks likely that a project or piece of work will affect people’s personal information.
- Notify the Information Commissioner’s Office and – in some cases the people concerned – if we suffer a serious data breach.
- And appoint a Data Protection Officer to be the go-to person on data protection issues.

SLIDE 6

TIMING: 3 MINUTES

- Be aware of the jigsaw effect: If you've got 2 or 3 bits of information, which, when you put them together, can be used to identify an individual (otherwise known as 'breadcrumbs'), that is all counted as personal information.

For example:

A vehicle registration number, which can be used by the DVLA to identify individuals, to match against names and address.

- If you take something like your vehicle registration or license plate on your car, to you and me it probably doesn't mean very much.
- But if you were the DVLA, then you've got the name, and the address, and a record of points against the license and the license plate.
- That's all personal information.

PRESENTER INSTRUCTIONS: PRESS FOR NEXT PART OF SAME SLIDE – RIGHT-HAND SIDE (SPECIAL CATEGORIES)

The Act provides a separate definition for "sensitive personal information".

There's a special category of personal information (**sensitive personal information**)

- This includes things like: health information, biometric and health data, trade union membership, religious or philosophical beliefs; racial or ethnic origin, criminal offences
- This is information we have to be especially careful with.

For example:

- For example, in December 2009 documents containing mental health records relating to 1,970 patients were reported missing. It appeared they were lost during transit with an external courier.
- In another example, a memory stick containing social services information concerning 40 children was found in a public street in Stoke-on-Trent.
- Marks & Spencer was found to have failed to protect data when an unencrypted laptop containing the personal pension details of around 26,000 M&S employees' was stolen.

SLIDE 7

TIMING: 3 MINUTES

PRESS RETURN FOR EACH NEXT PART OF THIS SECTION ON THE SLIDE

So, what are the core principles of GDPR?

Within the GDPR, there are some key principles that we need to adhere to in handling people's personal information.

1. Lawfully, fairly and in a transparent manner:

- We have to work in compliance with the law, in a way that is fair to those whose personal information we hold.
- And we need to be clear and transparent about what we are using the personal information for.

For example:

- You may have been getting emails from agencies or websites you've signed up to previously, asking you to consent to continue to be contacted by them for the purposes of sending information, e-mails, marketing etc.
- This presents a great, if one-off opportunity, to rid yourself of a good chunk of junk mail in that unless you specifically give your consent these companies will have to remove you from their distribution list.
- Interestingly, in the case of Starbucks, they've decided simply to delete their entire customer database and start again, rather than going to the effort of seeking everyone's consent.
- Businesses have to be very specific about transparency, about what they're sending you, and the purpose they're using your information for.
- Previously you might have experienced a privacy notice on a website, written in small type, and which acted as a catch all for that company to use your data for a wide range of purposes.
- This is not acceptable under GDPR.

- The purpose has to be clearly stated, and specifically agreed to – e.g. you want to receive a newsletter, you want to receive marketing ... so companies have to be transparent.

SLIDE 8

TIMING: 20 SECONDS

2. Purpose limitation:

- We should only use the personal information we hold to fulfil the purpose it was originally collected for.

For example:

- So, for example, externally, if you provide your email address for a newsletter, you should only receive a newsletter, you shouldn't receive anything else.

SLIDE 9

TIMING: 2 MINUTES

3. Data minimisation:

We should only gather the personal information we really need to fulfil the original purpose, and no more.

For example:

- So again, if you're signing up to a newsletter on flower arranging, you'd expect to provide your email address.
- But you would not expect to be asked for date of birth, your national insurance number, then that's not necessary to send you the thing you've asked for.
- Another example is Oracle E-business and booking sick leave.

? QUESTION TO AUDIENCE:

So, who's ever booked a sickness in Oracle eBusiness?

- How long did it take you to find 'cold or flu' in the list of diseases?
- The available options list is taken from the international compendium of diseases and comprises 482 different conditions.

? QUESTION TO AUDIENCE:

Now, what does the business do with that specific information about this specific nature of your complaints, do you think?

- Say, on average, that across the UK, we have about 9 days of sickness each a year, that database has been going for 10 years, and there's, what, 40,000 of us in the company, roughly-speaking.

- So, you're talking about something like 3.6 million records of all of our individual information which is a) Very sensitive, as we saw, and b) Probably inaccurate, because how many of us actually take the time, or feel comfortable to declare the specific condition we're suffering from.
- This information is being collected and stored, with an associated cost – however, is it actually used for anything?
- Whilst the higher level 'Absence Reason' may be reported on, the nature of the individual conditions is not.
- The principle here is to only collect the information you really need; and only use that information for the purpose stated.

SLIDE 10

TIMING: 20 SECONDS

4. Accuracy:

- We need to ensure the information we hold on people is accurate and up-to-date, in order to properly support the purpose for which it's been collected.

Example:

- A friend of the Data Protection team was complaining that money for her student loan was being taken from her account, when it had been paid off a year ago.
- Turns out, after investigating, they had another person with the same name and had mixed them up. Keeping information accurate is paramount.

SLIDE 11

TIMING: 2 MINUTES

5. Storage limitation:

- Only hold personal information for as long as you need it.

? QUESTION TO AUDIENCE:

- *How many of you have got spreadsheets that have been sat there for a number of years - on G-drives, for example?*
- *Do you know how many pieces of email we have in the company?*

Answer:

Network Rail currently holds around 2.9 billion bits of email.

? QUESTION TO AUDIENCE:

What types of emails should we keep?

Answer:

- There are some instances where we have to keep e-mail – for example, we have a legal obligation to keep all our chief executives' e-mails – however, this is the exception rather than the rule.
- There is therefore an argument to be had about the **value** of holding onto emails versus the **cost** of doing so.
- From a Data Protection point of view, the concern is that we are holding onto liabilities, in terms of the personal information that may be contained in those 2.9 billion e-mails.
- So if someone came and asked, 'I want to know what information you have about me...' – this could include e-mail information and could be a big search.

- **The principle here is to only hold personal information for as long as you need it, and then get rid of it.**
- **There is a corporate retention schedule which helps to define what these periods are.**

SLIDE 12

TIMING: 2 MINUTES

6. Integrity and confidentiality:

- We have to treat people's personal information with the appropriate security and protect it at all times.
- That means only allowing people access to the information who need it, and treating that personal information with the same respect we would expect our own information to be handled.

Example:

- **Have you ever been on a train and overheard a really juicy conversation?**
- Well, we've had examples where cases involving an individual was discussed in public places, both down the pub, and on a train.
- These conversations were overheard by a colleague of the person involved and this went to the ICO (the Information Commissioner) as a complaint.
- The point here is that 'personal information' doesn't just mean digital data, recorded information or printed information, it relates to **anything** involving an individual, so a conversation in a public place is equally applicable, and this is something the ICO will reinforce. It's not just about passwords and locks.
- **Think about how you would feel if your information was being discussed in public, information that you would expect to be kept private?**

SLIDE 13

TIMING: 3 MINUTES

- Depending on your role within the organisation, you may become familiar with these in time, but it is useful to touch on the basic principles behind this ‘legal basis’ with GDPR.

The above reflects the order in which the Processing Conditions are set out under GDPR.

If there is **one thing to remember and take away from this slide:**

The Legal Basis should not be considered in order of a–f.

We need to have a legal basis for every processing activity we carry out.

Legal Basis articles below, with examples of each.

- **Performance of a contract –**
 - As employees, our personal information is processed by our employer in order to pay us, for example.
- **Protecting the vital interests of a data subject, or someone else –**
 - This is when information is needed to protect the interests of an individual, or someone else, in a life or death situation.
- **Compliance with a legal obligation –**
 - An employer has legal obligations to governmental bodies such as HMRC in terms of tax information for example
- **Performance of a task carried out in the public interest –**
 - Does the processing relate to any functions, duties or powers vested in Network Rail via the Railways Act 1993 – does it relate to the running and operating of the railway infrastructure?

The two to avoid if possible from this list are:

- **Consent** – should be freely given, and means offering individuals real choice and control including the right to withdraw their consent at any time.
- Consent is not applicable in an employment context as there is an imbalance of power between the employer and employee, and is therefore not a reliable legal basis, because it can also be freely withdrawn.
- **Legitimate interests** –
 - There may be instances where this legal basis is justified **but only** if the processing activity falls outside of Network Rail's 'tasks' as a public authority. An example might be compiling directories of work e-mails for the purpose of distributing reports, maintaining business continuity etc.
 - We would recommend that business areas record their legal basis for processing.
 - **If you have any queries, then contact the data protection team.**

SLIDE 14

TIMING: 3 MINUTES

? QUESTION TO AUDIENCE:

What personal information are you aware of that you hold, that you deal with, that you manage?

And, the second question, given what we've discussed so far, where might you have concerns about how this information is being handled?

Prompt examples:

- CVs
- Rosters and rotas
- Birthday lists
- Spreadsheets with employee details
- Non password protected documents
- Photos and images
- We're all accountable, in some way, shape, or form: we will be handling personal information.
- Maybe that's in a big way, maybe it's in a small way, but we all have accountability.

SLIDE 15

TIMING: 20 SECONDS

Our goal is to build up a network of Data Protection Leads who can act as a first point of contact for data protection queries and lead activities to mitigate risk and encourage the organisation to get really good at data protection.

? QUESTION TO AUDIENCE:

Would you like to be a lead for data protection in your part of the business?

If so, please get in touch with Kerryanne Delbridge (contact details on the last slide), as we are building this network up and will be in touch with further information.

SLIDE 16

TIMING: 15 SECONDS

<https://haveibeenpwned.com/>

This is quite interesting.

- So, this is a website you can visit to see if your email address has been compromised at any point.
- You can have a look and see if your personal, or your work, or any one of the email addresses you hold, has been compromised.

SLIDE 17

TIMING: 1 MINUTE

- This is the result from Jeremy Bullock's (GDPR Readiness Programme manager's) personal email address.
- So he has three listings, but you'll see for yourselves what listings you might have.

Example:

- LinkedIn, May 2016, LinkedIn had 164 million email addresses and passwords exposed.
- They were originally hacked in 2012, but they only came to light, four years later in 2016, for sale on a dark market website.
- Change your passwords often, to reduce the risk of your personal information being exposed.
- So, just shows the activity that's going on in the background.

- Various other things we watched on the breaches film earlier - if you're aware of the Uber breach, and Yahoo!
- They reckon that all 3 billion of their subscribers were affected in some way or another.
- And Uber had personal information, including credit card details, stolen, and they paid the hackers to delete the data; but if they ever did, who knows.
- So, there's a lot of that stuff going on in the background. You see it come to the surface every now and again, but it is happening.

SLIDE 18

TIMING: 3 MINUTES

Example:

- Recently, the Information Commissioner's Office, the regulator, fined 13 large charities a total of around £200,000 for a practice known as '**wealth profiling**'.
- When people donated to the charities in question, teams would begin researching their backgrounds, finding out:
 - where they lived
 - what the value of their house was
 - and any other information they could find
- They did all this to work out how wealthy they were, and to target them with more marketing
- The Information Commissioner's Office ruled against the charities because donors would not have **reasonably expected** their personal information to be used in this way.
- They were enforced against, the ICO fined them collectively, 13 charities, £200,000.
- They said it would have been ten times more, except for the fact that they were charities and therefore they didn't want to impede on their work.

? QUESTION TO AUDIENCE:

- *Imagine how you would feel if that happened to you?*
- *Would you feel disappointed?*
- *Perhaps even betrayed?*

SLIDE 19

TIMING: 2 MINUTES

Has Network Rail ever had to notify the ICO of a data breach?

- Yes, the most recent example is in 2016.
- An office was being cleared out, and a variety of papers had been put in a paper recycling wheelie bin, in a loading bay within that building.
- However the bin was open and full to overflowing, with papers all over the ground.
- These included a variety of documents, including those containing personal information, such as CVs, interview notes etc
- The gate was open, anyone could have accessed that area.
- Fortunately, a member of Network Rail staff found it, and reported it to the data protection team, who took the necessary action to secure the information and to mitigate any risk.
- The Data protection team notified the ICO. They came and did an investigation and they gave the business some recommendations.
- This is known as a data breach and the person who discovered the documents followed our guidance, and escalated the issue to the data protection team who – in this case - notified the Information Commissioner's Office
- On this occasion the regulator decided not to take formal action, but that might not always be the case.

? QUESTION TO AUDIENCE:

- **Imagine how you would feel if your personal information was left lying around on the floor?**
- **Would you be anxious? Or feel let down?**

- One of the key points here, is that it's not just about electronic information.
- This is as much about paper-based, or video, or voice recordings as well.

SLIDE 20

TIMING: 1 MINUTE

You'll be aware of the Facebook incident.

[Case study example which was played in the Breaches film earlier]

- An app that allowed Cambridge Analytica to access many more times the information of people than the ones who signed up for the app.
- Key point: The ICO sought a warrant to investigate Cambridge Analytica's premises, and they enforced that warrant, went in, searched their servers, searched their files to get the evidence they needed of what they were doing.
- Cambridge Analytica has now closed their UK and US operations.
- This highlights the powers of the ICO to intervene if they have concerns about how personal information is being managed or used.

SLIDE 21

TIMING: 2 MINUTES

- Under GDPR, we have **just 72 hours** to notify the Information Commissioner's Office of any loss, breach of personal information.
- Under GDPR, the Information Commissioner's Office has the ability to levy a **fine of up to 4%** of any company's global annual turnover.
- For Network Rail, that could amount to a sum **in excess of £200 million pounds**.
- **A fair question is 'how likely' are the ICO to levy that kind of fine?**
- They have stated clearly that they want to work with businesses to do the right thing and prefer the 'carrot rather the stick'.
- The bigger risk for us is perhaps reputational.
- As a business a lot of effort has been made to build our relationship with government.
- Now that we are on the public books, as an arm's length body, any significant breach could significantly damage our reputation, both with the government, our own employees, and perhaps, the wider public.

Good data protection brings benefits to our business, as well as our customers - it:

- encourages us to act in a fair and transparent way – increasing public confidence and improving our reputation
 - helps to improve the quality of the information we have and improve our records management – increasing business efficiency and performance
 - keeps us alert to the security of our information and data – reducing risk

SLIDE 22

TIMING: 2 MINUTES

- The amount of data we hold in the company, about 4.5 peta-bytes.
- That's quite reasonable for our size of the business, but it's still a lot of information.
- A good chunk of that, is in unstructured data - V-drives, H-drives...
- Think of it – how many times do you e-mail a spreadsheet to a group? And what do each of those individuals most likely do with it? Save a local copy. If that's a 10MB spreadsheet, saved 10 times, that's 100MB gone in one instance. Then think if that spreadsheet holds personal information...

Example:

It's a lot of data, and with increased data volumes comes increased risk...

- A cascade briefing was recently held with a route and the next day, the data protection team received a phone call to say that there was a file which had been found on SharePoint.
- The folder was open to anyone to access, and the file contained c.36,000 employees' salaries and bonus information from two years ago.
- After investigation, we found that no one had accessed it, and fortunately neither had it been sent anywhere via e-mail.
- However, anyone could have accessed this file – with further consequences.

SLIDE 23

TIMING: 30 SECONDS

- The more clarity we have on what information we hold, why we hold it, where it's stored, and who we share it with, the more able we are to make quick and effective decisions.
- This will help us to be a better business, which is better for us, better for our customers, and better for the public at large.

- **You're aware of Lean methodologies?**

- So, if you think about the principles we were talking about, only gather what you need, only do what you said you were going to do with the information, and only hold it for as long as you need it, actually that fits really nicely with Lean.
- Because if you think about value, this is defined as what the customer/recipient wants.
- Anything that sits outside of this is waste.

Example:

- So, for example, if we gather 10 columns of information on a spreadsheet, but only two of those columns are adding any value, let's not gather the rest as this is unnecessary, and potentially presents a problem if this includes personal information.

SLIDE 24

TIMING: 2 MINUTES

The GDPR gives individuals (data subjects) specific rights.

Example:

One example is the right of access. Anyone has the right to ask a company to know all the information that company holds on them. An example is a journalist who submitted a 'Subject Access Request', as it is formally known, to the dating app company Tinder.

? QUESTION TO AUDIENCE:

How many pages of information do you think this person received in return?

Answer:

800 pages!

This included, the journalist said "...information such as my Facebook 'likes'; links to where my Instagram photos would have been; my education; the age-rank of people I was interested in; how many Facebook friends I had; when and where... every single one of my matches happened..."

Examples:

Another example is the 'Right to erasure', or the right 'to be forgotten'. It is important to note however, that just because this right exists, doesn't mean it will automatically be complied with. For example, there may be other legal reasons this right cannot be acted on, such as the company having a contract and therefore a legal obligation to continue paying you.

An interesting example, is the last one, not so much an issue for NR at the moment, but interesting just the same - the right to have a human being review a machine-made decision.

For example, if you apply for a loan and the ‘computer says no’, then if that decision was automated, i.e. made by an algorithm, you have the right to ask for a human being to review that decision and ensure it is correct.

SLIDE 25 – SECTION 1.

TIMING: 20 SECONDS

1. You're accountable

- Network Rail handles lots of personal information every day, from CVs to CCTV images and contact details of colleagues, customers and suppliers.
- We're all accountable for how we handle personal information.
- We should consider the privacy of others.
- Respect other people's personal information and treat it carefully – think about what impact it might have to someone - we are all accountable.

SLIDE 26 – SECTION 2.

TIMING: 20 SECONDS

2. P.L.A.N

- P.L.A.N means **P**roportionate, **L**awful, **A**ccurate and **N**ecessary.
- Review and document your business area's processes to ensure you're fully aware of what personal information you hold, why you're processing it, how long it should be held, where it came from, who you share it with and why.

SLIDE 27 – SECTION 3.

TIMING: 20 SECONDS

3. It applies to projects and programmes

- Use the data protection impact assessment (DPIA) to comply with ‘privacy by design’. *[More about the DPIA coming up shortly...]*
- The DPIA assesses the privacy risks of a project or programme and provides colleagues with the confidence that they are creating a compliant system for their work.

SLIDE 28 – SECTION 4.

TIMING: 20 SECONDS

4. Suppliers and third parties are involved

- Contractual arrangements and clauses need to be up to date and the processes around them must be compliant.
- Completing a Supplier DPIA can help teams to review how contracts are managed currently and how they’ll need to operate under GDPR.

SLIDE 29 – SECTION 5.

TIMING: 20 SECONDS

[MORE DETAILS ON SLIDE 34, SO KEEP THIS SLIDE BRIEF]

5. There are resources to help you

- The 'Data Protection Essentials' e-learning module is available via the (new) Network Rail Learning site:
<https://learning.networkrail.co.uk/auth/saml/login.php>
- Policies, the data protection impact assessment template, guidance and films can be accessed via the Data Protection Connect page.
- If you handle personal information, read the data protection handbook, and join the 'Data Protection & GDPR' Yammer group to join the conversation.

PROMPT:

Remind and prompt for the completion of the 'Data Protection Essentials' e-learning training, available on the (new) Network Rail Learning site.

<https://learning.networkrail.co.uk/auth/saml/login.php>

PROMPT:

- **IMPORTANT NOTE ABOUT THE E-LEARNING MODULE ACCESS:**
- (SEARCH UNDER THE: **Corporate and Social Responsibility heading**)

The business is improving access to all of Network Rail's eLearning training with a new platform that is **now available** to all Network Rail employees. The new platform, which **replaces the current eBusiness suite**, is easier to access and more reliable than our old system.

Saving time

Any associated Oracle competences will be updated automatically when colleagues successfully complete eLearning courses.

More user-friendly

The new system is also simpler to use. Access has been set up automatically for all existing staff and new employees will be automatically added to the system when they join the company.

Those who already have an individual Network Rail IT account to log into a laptop or desktop computer can use the same username and password to access their eLearning.

Those who don't have an IT account of their own can log in using their employee number, and a unique password.

Mobile compatibility

Colleagues who don't have a laptop or PC can access eLearning on mobile devices, enabling them to undertake online training whenever and wherever they like.

SLIDES 30-32 [PRESS RETURN TO SEE THE TYPES OF SCORING]

TIMING: 1 MINUTE

Are there any tools available to help me?

Yes, the Data Protection team at Network Rail have developed a tool called the **data protection impact assessment**.

- This is a series of questions that will help you to assess the risk involved in any programme, project, activity, process, or system that you're looking at.
- The outcome of this is a score.
- The score will tell you whether the activity or the process or system is high risk, or low risk, and it will help you to think about what can be done to mitigate that risk when necessary.
- One purpose of a DPIA is that it helps projects identify and therefore mitigate against risks – in addition it acts as evidence, an audit trail of the considerations the project took into account at the development stages.
- ‘Privacy by design’ is a concept within the current Act....using the DPIA early on in projects can help prevent issues later down the line.
- Projects are expected to undergo at least two iterations of the DPIA, the first to identify any risks, the second to reflect the mitigating steps taken to reduce the risk.

SLIDE 33

TIMING: 30 SECONDS

Data Protection and Close Calls

- 'Data Protection' is being added under our Close Call Category drop down option.
- There will be a new Security category, and as a sub-category, 'Data Protection' will be listed.

In all cases where we personal information is being handled, we should ask ourselves the following questions:

- Do I need to store/use this personal information?
- Have I thought about where it should be stored?
- Am I only giving access to those who need it?
- Do I tell people why I need their information and what I will use it for?
- Do I understand people's right to privacy?
- Will a project or piece of work affect someone's personal information?

Take five (suggestion – you could use this as a Take 5 for safety discussion in a future meeting):

- Discuss how you handle personal information, that might be in a project you're running or as a recruiting manager for example.
- Do you have concerns about how you're handling that information?
What can *you* do differently now/in future to make sure you're treating it in a fair, accountable and safe way?
- Then share your thoughts with the group.

SLIDE 34

TIMING: 2 MINUTES

Actions to take next:

1. Complete the **'Data Protection Essentials' e-learning module**
(search 'Data protection' on the Oracle eBusiness suite;

OR the new Network Rail Learning site:
<https://learning.networkrail.co.uk/auth/saml/login.php>)
2. Join the Yammer group
'Data Protection (& GDPR)'
Sign up for Yammer and roadshow clinics
3. Search **Connect / Data Protection**
Policies, the data protection impact assessment templates, guidance and films
4. Read our **Data Protection handbook**

Available as a PDF on the Data Protection page on Connect

Printed copies available from the Data Protection team
5. **Watch/download these 3 films:** (Connect/Data Protection)
 - a) GDPR at Network Rail film (5 minutes)
 - b) Breaches film (5 minutes)
 - c) ICO film (3 minutes)
6. Do **seek support** from the DP team data.protection@networkrail.co.uk

SLIDE 35

Key contacts

IMPORTANT NOTE TO PRESENTER:

[Please email Kerryanne Delbridge once you have completed the briefing for our records.

See the ‘Presenter instructions’ for further details.]

SLIDE 36

Remind and prompt for the completion of the 'Data Protection Essentials' e-learning training, available on the (new) Network Rail Learning site.

<https://learning.networkrail.co.uk/auth/saml/login.php>

PROMPT:

- **IMPORTANT NOTE ABOUT THE E-LEARNING MODULE ACCESS:**
- (SEARCH UNDER THE: **Corporate and Social Responsibility heading**)

The business is improving access to all of Network Rail's eLearning training with a new platform that is **now available** to all Network Rail employees. The new platform, which **replaces the current eBusiness suite**, is easier to access and more reliable than our old system.

Saving time

Any associated Oracle competences will be updated automatically when colleagues successfully complete eLearning courses.

More user-friendly

The new system is also simpler to use. Access has been set up automatically for all existing staff and new employees will be automatically added to the system when they join the company.

Those who already have an individual Network Rail IT account to log into a laptop or desktop computer can use the same username and password to access their eLearning.

Those who don't have an IT account of their own can log in using their employee number, and a unique password.

Mobile compatibility

Colleagues who don't have a laptop or PC can access eLearning on mobile devices, enabling them to undertake online training whenever and wherever they like.

SLIDE 37

THANK YOU – from the Data Protection team

PRESENTERS – NEXT STEPS, PLEASE:

- 1. Email: Kerryanne Delbridge that you've held a briefing, how many people attended, with any further queries from your team.**
- 2. Follow the 'Presenter instructions' about what to send team members who were unable to attend.**