



Research Policy & Standards Webinar

Stay up-to-date and within the rules

-
- Debrah Harding, FAcSS, FRSA
 - Managing Director, MRS
 - [#TweetMRS](#)



1

Domestic developments

Debrah Harding
Managing Director

2

International and
European updates

Kaleke Kolawole
Policy Manager

3

Codeline hot topics and
other new MRS guidance

Julie Corney
Standards & Compliance
Manager

Employment Rights Bill Update



- The Employment Rights Bill is also making its way through the Parliamentary process
 - It is currently in the House of Lords committee stage following the second reading
 - MRS has met with DBT to express concerns regarding the proposals for zero hour contracts and whether these will affect flexible worker contracts used for interviewers
 - MRS has been liaising with other business groups such as the CBI, Federation of Small Businesses and the Advertising Association to ensure that the research sector's concerns are reflected in lobbying efforts by others – to enhance the message
 - DBT has acknowledged the issues raised by MRS and the practical difficulties of shoe-horning interviewer workflows into guaranteed hours contracts
 - The secondary legislation will provide the necessary clarity and MRS is working to influence DBT regarding the scope of the secondary legislation
 - There is nothing for employers to do now but if you do use zero hour/flexible worker contracts have a look at interviewer working patterns, and if these were to migrate to guaranteed hours, and how this might affect your business
-

Data Use and Access Bill



- The new Data Use & Access (DUA) Bill continues its progress through Parliament
 - The Bill has had its report stage, and the third reading took place on 7th May
 - The consideration of common amendments and reasons is due to take place today, 12th May
 - MRS is continuing to make representations on the scientific research provisions, and particularly to have adherence to the MRS Code of Conduct by MRS Company Partners and MRS members recognised as an appropriate 'ethical, legal and professional framework' as per the Bill
 - The Bill is now very close to being finalised and gaining Royal Assent
 - Once finalised MRS will be issuing a guidance note on the key points from the Bill – but fundamentally the practice of research will remain unchanged as a result of the Bill
 - The main impact will be legislative clarity for activities such as scientific research
-

Data Use and Access Bill – other topics



- MPs are proposing a new clause that in certain circumstances would raise the age for processing personal data in the case of social networking services from 13 to 16
 - MPs also propose that parents of a deceased minor could obtain that child's social media data without a court order, subject to privacy safeguards for third parties
 - Amendments are also proposed for AI and copyright - a new clause would require web crawlers and general-purpose AI models with UK links to comply with UK copyright law across all stages of AI development
 - Another proposed new clause would grant the Information Commissioner enforcement powers to ensure compliance with AI and web crawler transparency rules, including penalties for breaches
-

Data Use and Access Bill – EU adequacy



- On 18 March the European Commission proposed to adopt an extension to the UK's adequacy decisions for a period of six months until 27 December 2025
 - The extension is due to the DUA Bill
 - Once the new Bill has been adopted, the EU Commission will assess this new legal framework and decide on its adequacy
 - The European Data Protection Board will then issue its Opinion before an approval is sought from representatives of EU countries
-

ICO Anonymisation Guidance



- In March 2025 the ICO published its Anonymisation and Pseudonymisation guidance
 - MRS input into the creation of this ICO guidance
 - This guidance help develop understanding of anonymisation techniques, their strengths and weaknesses, and the suitability of their use in particular situations
 - The guidance also:
 - explains what the ICO means by anonymisation and pseudonymisation
 - details how this affects data protection obligations and responsibilities
 - discusses what should be considered when anonymising personal data
 - provides good practice advice anonymising personal data
 - discusses technical and organisational measures to mitigate the risks to people and their data when undertaking anonymisation or pseudonymisation
-

ICO Anonymisation Guidance – anonymisation points to note



- Anonymisation ensures that the risk of identification is sufficiently remote to minimise the risks to people arising from the use of their information
 - Identifiability is a wide concept - a person can be identifiable from many factors that can distinguish them from someone else, not just a name
 - Identifiability exists on a spectrum - when assessing whether someone is identifiable, take into account the “means reasonably likely to be used to enable identification”
 - There are likely to be many borderline cases where judgement based on the specific circumstances of the case will be required
 - Purely hypothetical or theoretical chance of identifiability does not need to be taken into account, rather, what is reasonably likely relative to the circumstances
 - Consider both the information itself, and who may get (or want to get) access to it
 - Use robust techniques to reduce the higher risk of unauthorised personal data disclosure compared to intentional and controlled data release to known recipients
 - Consider potential unauthorised access by people (e.g., hacking or the actions of rogue employee)
 - Apply a “motivated intruder” test is a good starting point to consider identifiability risk
 - Review risk assessments and decision-making processes regularly
-

ICO Anonymisation Guidance – pseudonymisation points to note



- Pseudonymisation refers to techniques that replace, remove or transform information that identifies people, and keep that information separate
 - Pseudonymised personal data is in scope of data protection law
 - Pseudonymisation can help to reduce the processing risks by:
 - implementing data protection by design
 - ensuring appropriate security
 - making better use of personal data (e.g., for research purposes and general analysis)
 - Take care not to confuse pseudonymisation with anonymisation
 - Pseudonymisation is a way of reducing risk and improving security - it is not a way of transforming personal data to the extent the law no longer applies
 - The DPA 2018 contains two criminal offences that address the potential harms that result from unauthorised removal of pseudonymisation
 - There are many pseudonymisation techniques - some will help you achieve pseudonymisation as defined by the law - others may not, but can still be useful technical measures from a security perspective
-

DSIT: Cyber Governance Code of Practice



In April 2025, the Department for Science, Innovation and Technology (DSIT) launched a **new Cyber Governance Code of Practice** to help directors and company boards protect their organisations from growing cyber threats

The package includes:

- The Cyber Governance Code of Practice – with key actions for business leaders
- Online training and a detailed Board Toolkit
- Support for small businesses via the NCSC's Small Business Guide and Cyber Local funding scheme

Key Measures in the Code

- Establish a cyber strategy that supports business resilience and growth
- Promote a cyber-secure culture across all levels of the organisation
- Develop and maintain incident response plans to respond quickly to cyber breaches

The guidance is tailored to support both large firms and SMEs, addressing major gaps such as:

- One-third of large businesses not having a formal cyber strategy
 - Nearly half of medium firms lacking an incident response plan
-

DSIT: Cyber Governance Code of Practice



Context and Support

- 74 percent of large businesses and 70 percent of medium-sized firms experienced a cyber breach or attack in the past year
- Cyber threats cost the UK economy nearly £22bn annually between 2015 and 2019
- Support for Small Businesses:
 - The NCSC's Small Business Guide offers simple actions to improve online security
 - The Cyber Local scheme provides tailored funding to boost regional cyber skills

Future Legislation

- The announcement follows recent plans to introduce cyber security legislation later this year
 - These proposals aim to:
 - Protect supply chains, critical national services, and IT service providers
 - Improve cyber resilience in hospitals and energy suppliers
 - Further secure digital services crucial to economic growth
-

Some data breaches – DPP Law LLC



DPP Law LLC

- DPP is a law firm, headquartered in Bootle, England which employs fewer than 250 staff and has offices in Birmingham, Bootle, Liverpool, London and Tolworth
- On 4 June 2022 DPP's email server stopped working and staff had no access to DPP's IT network
- DPP's in-house IT manager established that all files across its servers had been corrupted and DPP's external IT supplier believed that DPP had suffered a ransomware incident, despite not receiving any payment demands
- The National Crime Agency contacted DPP to advise them that three folders of DPP's data, totalling 32.4Gb, had been published on the dark web
- This included court bundles, PDFs, Word documents, photos and video (including police body cam footage) relating to DPP's clients and experts instructed to give evidence in legal proceedings to which DPP's clients were a party
- 43 days after the Cyber Incident, DPP reported the personal data breach to the Commissioner
- DPP were unaware that the loss of access to personal data constituted a personal data breach and therefore that they were required to notify the Commissioner about the Cyber Incident
- The personal data of 791 individuals (clients and experts) were exfiltrated by a threat actor and posted on the dark web

Points to note:

- The fact that the Cyber Incident took place is not, in and of itself, sufficient to make a finding that DPP has infringed the security requirements in UK GDPR
 - The infringements of UK GDPR occurred because the relevant processing was not carried out in a manner that ensured appropriate security of the personal data of DPP's clients and experts, including protection against unauthorised processing, and using appropriate technical and organisational measures
 - In particular, DPP failed to adopt the principle of least privilege and failed to regularly audit administrative accounts on its network
 - A financial penalty of £60k was incurred as a result
-

ICO Social Media and Video Sharing Platforms Investigation



- In March the ICO launched three investigations into TikTok, Reddit, and Imgur regarding their handling of children's personal data
 - The investigations aim to determine whether these platforms comply with UK data protection laws when dealing with child users
 - The ICO is investigating how TikTok uses personal information of 13–17-year-olds to make recommendations and deliver suggested content
 - The focus on Reddit and Imgur investigations is on how these platforms assess and verify the age of their UK child users to ensure adequate protections are in place
 - The ICO is investigating whether any of these platforms have violated data protection laws
 - Since the introduction of the Children's Code in 2021, the ICO has pushed for stronger protections on social media and video-sharing platforms
-

ICO Social Media and Video Sharing Platforms Investigation



Other Recent regulatory interventions

- X (formerly Twitter) stopped serving ads to users under 18 and removed geolocation sharing for minors
- Sendit and BeReal restricted the sharing of children's location data
- Dailymotion introduced new privacy and transparency measures
- Viber disabled personalised advertising for child users

Next Steps

- The ICO will continue to push for stronger child data protections and take further action where platforms fail to comply
 - The ICO and Ofcom will collaborate to enforce the Online Safety Act and ensure children's data is safeguarded
-



Meta UK Settlement

- Meta and an individual who challenged the company for serving targeted advertising based on her online behaviour on Facebook have settled the case out of court
 - Ms O'Carroll claims a victory as Meta has committed to stop processing her personal data to serve her with bespoke ads, and the case may set an important precedent
 - The ICO intervened in the O'Carroll vs Meta case to assist the Court with the application of the right to object under the UK GDPR. It said in a statement:
"People have the right to object to their personal information being used for direct marketing, and we have been clear that online targeted advertising should be considered as direct marketing"
 - The ICO says that Ms O'Carroll has an absolute right to object to the processing of her personal data and related profiling for the purposes of online targeted advertising where that processing and profiling are for direct marketing purposes
 - Meta is considering introducing a 'Consent or Pay' model in the UK – and the ICO has indicated that this is possible as long as companies give users "meaningful control"
-

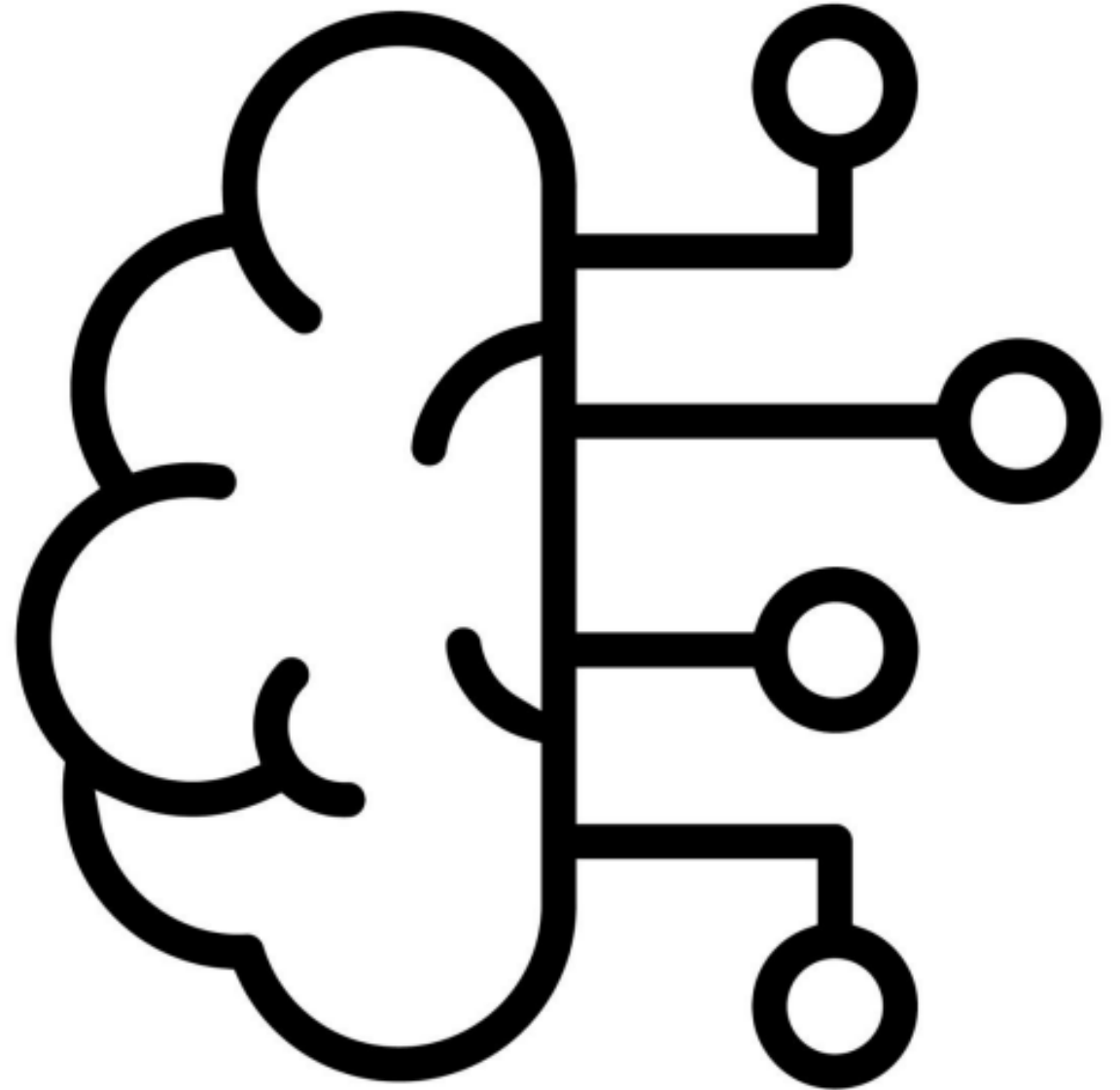
Campaign for Better Data



- On 1st May 2025, MRS launched the Campaign for Better Data, providing guidance and training to help the sector strengthen and evolve the quality of the evidence it produces and reinforce public trust in research
- With the government setting out to establish the country as a world leader in AI, there is a significant opportunity for the £9 billion UK research sector to boost its efficiency and focus efforts where human insight can generate most value
- However, misinformation poses a growing risk which AI has the potential to exacerbate
- Against this backdrop, MRS is providing new resources to help those in research to create even better data
- It is calling on the research sector to continue to be vigilant and hone its skills to further fortify data accuracy and quality, ensuring the research sector is future-proofed
- <https://www.mrs.org.uk/topic/campaign-for-better-data>



Update of the MRS AI and Related Technology Guidance



MRS AI and Related Technologies Guidance



- In April 2025 the updated MRS AI and Related Technology guidance was issued
 - The second iteration of this document first launched in November 2023
 - This guidance applies to all MRS members and MRS Company Partners and should be read in conjunction with the MRS Code of Conduct
 - The guidance includes:
 - An update on the UK AI legislative approach
 - An update on the implementation of the EU's AI Act
 - Some refinement and clarification of the existing requirements
 - Addition of extra commentary for many of the rules to help to illustrate the application of the requirements
 - The addition of new requirements for data creation and use including synthetic data
-

MRS AI and Related Technologies Guidance

– Data Creation & Use



- Practitioners must obtain participant consent for any personal data used to enhance AI and related technologies, including in the creation of synthetic data models.
Comment: In addition to consent, participants should anonymise data before it is used in AI and related technologies to protect participants and reduce the likelihood of harm .
 - Practitioners must obtain client consent for the use of AI and related technologies in data creation e.g., the use of synthetic data techniques. When obtaining consent, practitioners must include a clear description of purpose, where in the process AI and related technologies are used, and the abilities and limitations for the use of any proposed AI and related technologies.
 - Practitioners must maintain records detailing how AI and related technologies are used in data creation including how data is generated (e.g., prompts) and combined, how bias and errors are mitigated, the frequency of data updates/refresh and the source of any training data.
Comment: For example, when synthetic data is used, including when it is combined with non-synthetic data in the same dataset, each synthetic data element would need to be clearly identifiable.
-



International Update

Kaleke Kolawole



US: Texas Responsible Artificial Intelligence Governance Act passes House



-
- On April 23, 2025, House Bill 149, known as the Texas Responsible Artificial Intelligence Governance Act, was passed by the Texas State House of Representatives.
 - The Bill aims to regulate AI systems by imposing prohibitions and requirements, including rules on AI regulatory sandboxes and biometric identifier usage. The bill mandates clear disclosure when AI systems interact with consumers and prohibits AI systems from inciting harm, infringing rights, or discriminating unlawfully.
 - Enforcement is exclusively handled by the Texas Attorney General, with penalties for violations, and the bill is set to enter into force on January 1, 2026.
 - Some of the provisions in the Bill include:
 - Application: Any person who promotes, advertises, or conducts business in Texas
 - Biometrics: The presence of an image or other media containing a biometric identifier on publicly available sources does not imply consent for the capture or storage of that biometric identifier for commercial purposes.
 - If enacted, the Bill enters into force 1 January 2026
-

FRANCE: CNIL RECOMMENDATIONS



-
- The French data protection authority, CNIL, announced its 2025 work program focusing on GDPR compliance support for professionals.
 - The program includes creating practical sheets on AI and GDPR interactions, benchmarks for sub-processor processing standards and health data processing, guidelines on data retention in commercial activities, and recommendations on multi-device consent, email pixels, and age-based data processing.
 - CNIL outlined the following projects:
 - additional practical sheets relating to artificial intelligence (AI), focusing on legitimate interest, the interaction of the GDPR and AI, and deploying AI;
 - establishing a benchmark for evaluating the standard of processing by sub-processors, following a public consultation in 2024;
 - establishing benchmarks for processing health data, following a consultation in May 2024
 - establishing benchmarks regarding the use of algorithms by banking and credit institutions;
 - publishing guidelines on retention periods for data commonly processor in commercial and marketing activities;
 - draft recommendations on multi-device consent, the use of pixels in emails, and processing the personal data based on the age of data subjects.
-



China: CAC on SYNTHETIC DATA

- The Cyberspace Administration of China (CAC), in collaboration with multiple ministries, released new regulations and standards on March 14, 2025, to manage the identification of synthetic content generated by artificial intelligence (AI).
 - These include Measures for the Identification of Synthetic Content and a national standard for identifying such content in cybersecurity technology. The measures mandate explicit and implicit identification of AI-generated content, adherence to existing regulations, and prohibit tampering with content identification.
 - According to the CAC, the measures for identifying synthetic content generated by AI include:
 - Explicit Identification: Clearly visible identification added to synthetic content or interactive scenes, presented as text, sound, or graphic
 - Implicit Identification: Identification embedded in the file data of synthetic content through technical measures, not easily perceived by users.
 - Additionally, the measures require:
 - Compliance with relevant regulations, including those for algorithm recommendation, deep synthesis management, and generative AI services.
 - Explicit identification for synthetic services provided by service providers under the deep synthesis regulations.
 - Implicit identification in the metadata of synthetic content files as per Article 16 of the deep synthesis regulations.
 - Implementation of technical measures for content dissemination by network information content providers.
 - The measure take effect September, 2025
-



SPAIN: Minor's Digital Protection

- Spain's Council of Ministers has submitted a draft law to Parliament aimed at protecting minors in digital environments.
 - The draft includes contributions from various Spanish organisations and the European Commission, and features provisions for minors' rights to protection and access to digital resources, parental control systems on mobile devices, health promotion guidelines addressing social media addiction, and a national strategy for digital protection of youth.
 - It also proposes amendments to existing regulations, introducing judicial powers to suspend harmful digital services, criminalising 'deepfakes' with abusive content, and mandating reporting channels for inappropriate content by major media entities and popular influencers.
 - **Key Provisions of the Draft Law by the Council of Ministers**
 - Protection and Access for Minors: Ensures minors have effective protection, truthful information, and equitable access to digital devices and connections.
 - Parental Control Systems: Mandates mobile device manufacturers to provide effective, free, and accessible parental control systems.
 - Health Promotion Guidelines: Requires relevant authorities to develop health promotion guidelines and programs, addressing potentially addictive behaviors related to social media.
 - National Strategy for Digital Protection: Obligates public authorities to develop a national strategy for protecting children and adolescents in the digital environment.
-



MRS Guidance update

Julie Corney



The European Accessibility Act (EAA)



The European Accessibility Act (EAA), which aims to improve the accessibility of products and services for people with disabilities within the EU, will come into force on June 28, 2025. The EAA applies to any organization that provides products and services to consumers in the EU, including businesses and public bodies in the UK. While the UK is not a member of the EU, it is still expected to comply with the EAA if it sells products or services to EU consumers.



The European Accessibility Act (EAA)

Key aspects of the EAA:

Scope:

The EAA covers a wide range of products and services, including digital products like websites and apps, and also physical products like ATMs and ticketing machines.

Compliance:

Businesses must ensure their products and services meet specific accessibility requirements, aiming for a minimum level of accessibility.



The European Accessibility Act (EAA)

Key aspects of the EAA:

Accessibility standards:

The EAA aims to harmonize accessibility requirements across the EU, potentially reducing costs and simplifying cross-border trade for businesses.

Impact on UK businesses:

While not directly bound by the EAA, UK businesses that sell products or services to EU consumers will need to ensure compliance to avoid legal and reputational risks.

Enforcement:

Failure to comply with the EAA could result in fines and other penalties, depending on the severity of the non-compliance.

The European Accessibility Act (EAA)



Businesses will benefit from:

- common rules on accessibility in the EU leading to costs reduction easier cross-border trading more market opportunities for their accessible products and services

Persons with disabilities and elderly people will benefit from:

- more accessible products and services in the market
 - accessible products and services at more competitive prices
 - fewer barriers when accessing transport, education and the open labour market
 - more jobs available where accessibility expertise is needed
-

The European Accessibility Act (EAA)



Products and services covered

The European accessibility act covers products and services that have been identified as being most important for persons with disabilities while being most likely to have diverging accessibility requirements across EU countries.



The European Accessibility Act (EAA)

The Commission consulted stakeholders and experts on accessibility and took into account the obligations deriving from the UN convention on persons with disabilities. These products and services include:

- computers and operating systems
 - ATMs, ticketing and check-in machines
 - smartphones
 - TV equipment related to digital television services
 - telephony services and related equipment
 - access to audio-visual media services such as television broadcast and related consumer equipment
 - services related to air, bus, rail and waterborne passenger transport
 - banking services
 - e-books
 - e-commerce
-

The European Accessibility Act (EAA)



What's the timeline for the EAA?





The European Accessibility Act (EAA)

Each member state is responsible for enforcement, which means they can appoint the body in charge of enforcement and decide penalties.

Penalties

Member states also oversee their own penalties for noncompliance, which should be “effective, proportionate, and dissuasive.”

Reporting noncompliance

Each member state must make it possible for consumers to report noncompliance to either the courts or the body in charge of enforcing the law in that country.

Both public and private organizations also must have the option of going to court or filing a complaint with the body in charge.



The European Accessibility Act (EAA)

How do I know if the EAA applies to my business?

Most businesses based in or offering services to European consumers are required to be EAA compliant. There is an exception in the act for “undue burden,” meaning a company doesn’t have to comply if it would change the nature of the product/service or if the company would be financially overburdened.

There’s also an exception for what the act calls “micro-enterprises,” which are companies with less than 10 employees and an annual balance sheet total not exceeding €2 million.

The European Accessibility Act (EAA)



How do I know if the EAA applies to my business?

There are a few specific instances that are exempt from compliance:

- Pre-recorded time-based media (e.g., videos) published before June 2025
 - Office file formats published before June 2025
 - Online maps, if essential information is otherwise provided in an accessible way
 - Third-party content that is not funded, developed, or under the control of an organization that must be compliant
 - Archived content that won't be updated after June 2025
-



The European Accessibility Act (EAA)

How can I make sure I'm EAA compliant?

You can't go wrong by starting with a general "Design for All" approach that ensures that your digital presence (and products) are usable by everyone.

To comply with EAA, businesses should implement various accessibility features, such as text-to-speech, keyboard navigation, and screen reader compatibility.

MRS is currently reviewing the existing suite of MRS guidance in this area to help support the membership in EAA compliance. If you have any questions in the meantime, please contact the MRS Codeline advisory service codeline@mrs.org.uk



Thank you

If you have any queries please
contact: codeline@mrs.org.uk