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

Debrah Harding
Managing Director

3

MRS guidance

Julie Corney
Standards & Compliance Manager

Zero Hours Contracts Consultation

- DBT published “Make Work Pay: ending one-sided flexibility – reforms of zero hours and similar contracts” on 2 June 2026

- The consultation seeks views on the detail, to be set out in regulations, of three measures in the Employment Rights Act 2025:

    - A right to guaranteed hours, where the hours offered reflect those worked by a qualifying worker during a reference period
    - A right to reasonable notice of shifts and of changes to them
    - Payment for shifts cancelled, curtailed or moved at short notice – these measures have not yet taken effect

Zero Hours Contracts Consultation

- MRS has written to the Prime Minister and the relevant Secretary of State setting out the sector's concerns about the implications of these proposals for flexible worker contracts
- MRS supports stronger worker protections, but argues the rules must be targeted at those 'exploited', not at legitimate flexible fieldwork contracts
- MRS argues research sector flexible worker contracts should be out of scope: engagements are project-based, with no fixed work pattern and no mutuality of obligation
- Work is only available when projects are commissioned, so businesses cannot guarantee hours – in scope, they would be paying interviewers when no work exists
- The current contracts benefit interviewers, who choose when and for whom they work, decline projects freely, and still receive holiday pay, SSP and SMP
- This flexibility sustains a field force of parents, carers, retired people and those in rural areas – the groups Government wants in work
- The proposals could result in a huge increase in administration costs with some projects becoming potentially unviable which could result in the quality of evidence falling
- Guaranteed hours would also remove the incentives that drive high response rates such as those required for government projects

- ***Next steps:*** MRS is gathering member input and will respond before the end of August deadline

Late Payments – Small Business Protections

- The Small Business Protections Bill (formally the Commercial Payments Bill) is at the Committee stage in the House of Lords
- Late payments cost the UK economy around £11 billion a year and are linked to 38 business closures every day
- The Bill introduces a 60-day cap on payment terms for large firms and mandatory interest at the Bank of England base rate plus 8%
- The Small Business Commissioner gains powers to investigate poor payment practices, adjudicate disputes and fine persistent late payers
- A requirement for boards or audit committees of persistently late-paying large companies to publish explanations of poor payment performance and steps to improve it

- ***Potential impact:*** benefits freelancers, sole traders and smaller research suppliers – larger agencies should review payment terms ahead of Royal Assent

DSIT Abolished – New AI Minister

- The Department for Science, Innovation and Technology (DSIT) has been abolished
- Some responsibilities move to an expanded Department for Business and Trade (DBT), creating a new Department for Business, Innovation, Science and Technology (DBIST); others move to the Department for Digital, Culture, Media and Sport (DCMS)
- A new AI Minister, Kanishka Narayan, has been appointed and will work from the Cabinet Office
- In parallel with this the Cabinet Office has announced the creation of a new AI Taskforce to direct the Government's overall AI strategy and lead work to transform public services and unlock growth and prosperity across the country

- ***Potential impact:*** policy ownership for data, AI and online safety is now spread across departments – watch for changes in consultation leads and points of contact

DSIT Consultations – Data Transfers, AI and Public Sector Data

- Before the department was abolished DSIT announced three consultations to inform future policy development:

    - **Call for evidence on international data transfers** which seeks stakeholder experience of the current system and views on areas most suitable for reform
    - This includes whether "partial" adequacy would be helpful for more countries where "full" adequacy might not be possible, and which aspects of Transfer Risk Assessments are challenging for organisations

    - **Call for evidence on data regulation** in the age of AI and other data-intensive technologies: seeks practical examples of how personal and non-personal data are used

    - **A further consultation covers the re-use of public sector data** and whether public bodies should charge above marginal costs for the re-use of public sector data

- ***Potential impact:*** an opportunity for the sector to shape reform of the transfer regime and AI-related data rules – MRS will be responding

Research Evidence – AI Economics Institute

- In June HM Treasury and DSIT established the AI Economics Institute (AIEI), a joint research organisation set up to build the data infrastructure, analytical capability and external relationships needed to assess AI's economic impacts
- The Institute will work in partnership across government, academia, civil society and industry
- It will work with HMRC and the ONS to explore what data could be made available for research, and will continue the Future of Work Unit's engagement with trade unions and businesses
- More than 20 major companies have signed up to share data on how they are using AI in the workplace, and an existing data partnership with LinkedIn will carry over to the Institute

- ***Potential impact:*** more public data being available to use for research and an opportunity for research businesses to contribute to the work of the Institute

The Charity Soft Opt-In

- The ICO has published final guidance on the "charitable purposes soft opt-in", within its updated direct marketing and electronic communications guidance
- The exemption was created by the Data (Use and Access) Act 2025, amending PECR, and took effect on 5 February 2026
- It allows charities to send electronic mail marketing for charitable purposes without prior consent, but only where the contact details came from the individual expressing interest in, or offering or providing support to, those purposes
- A simple means of opting out must be given when details are collected and in every subsequent message
- The Fundraising Regulator has since issued a guide on the soft opt-in and fundraising marketing, alongside the ICO's guidance

- ***Potential impact:*** charity clients may widen email contact strategies – genuine research remains outside PECR's direct marketing rules

ICO Strategy and Other Updates

- The ICO has issued a draft corporate strategy for consultation covering 2026 to 2028, prioritising children's data, AI, public sector data use and cyber resilience
- The ICO will transition to the Information Commission model under the Data (Use and Access) Act (DUAA) 2025, expected to be in place in the autumn 2026
- Earlier this year the current Information Commissioner resigned, and their replacement is being sought
- In parallel with this the Government has announced an independent review of the "…culture, accountability and governance of the ICO…"
- The DUAA complaints provisions (covered in the last quarterly update) came into force on 19 June 2026
- UK organisations must have a formal complaints process in place and individuals must first use an organisation's internal complaints procedure to resolve complaints

- ***Potential impact***: with the regime change there might be a shift in focus for the ICO – whatever the Government's Growth agenda is likely to require a 'pro-business' approach

ICO Annual Report 2025/26

- In July 2026, the ICO published its Annual Report covering what is expected to be the last full year of the ICO before it transitions to a statutory board
- The ICO concluded 62 UK GDPR investigations, up from 43 in 2024/25
- It issued eight fines totalling over £32 million, compared with two fines totalling around £4 million the previous year
- Data protection complaints rose to 76,743, from 42,315 – described by the ICO as a significant and sustained increase in demand
- Reported data breaches rose to 17,431, from 12,412, with reports highest in the health, education and childcare sectors

- **Point to Note:**

- The most common incident type remains sending personal information to the wrong person by email, post or fax – a reminder that basic operational controls matter as much as policy

Social Media Ban for Under-16s

- On 15 June the government announced that by spring 2027 it will be unlawful for children under 16 to hold social media accounts, following the Australian legislative approach
- The ban captures user-to-user platforms whose purpose is to enable social interaction and which allow users to post material, alongside algorithmic feeds – named platforms include Snapchat, TikTok, YouTube, Instagram, Facebook and X
- Messaging services such as WhatsApp and Signal are not intended to fall within the ban
- Exemptions include educational services, e-commerce platforms and music streaming
- The measures will be delivered through new regulations under the Online Safety Act 2023, using powers created by the Children's Wellbeing and Schools Act 2026, with legislation expected before Parliament by the end of the year
- First restrictions expected to be in effect in Spring 2027, with Ofcom asked to report within the first year on the extent of circumvention
- The move follows a wide public consultation, Ofcom enforcement of the Online Safety Act and ICO action on the Children's Code
- In addition, the G7 Digital Ministers agreed a first joint approach to protecting children online, covering digital literacy, AI chatbot risks and effective age assurance

Social Media Ban for Under-16s

The ban covers four main areas:

- Social media ban for under-16s: social media companies will be banned from offering their services to under-16s, with additional default restrictions on certain functions for 16- and 17-year-olds
- Restrictions on risky functions elsewhere: under-16s will be prevented from communicating with strangers and creating livestreams on other services, including gaming - these features will be switched off by default for 16- and 17-year-olds
- AI chatbot limits: chatbots whose primary purpose is to provide sexual relationships will not be available to under-18s; general-purpose chatbots will not be age-gated, but users will need to prove they are over 18 to access features enabling sexually explicit interaction
- Stronger age checks: companies will be required to use highly effective age assurance to identify under-16s, with more adults expected to verify their age as a result

- ***Potential impact:*** organisations should be alert to regulator's increased appetite to enforce in this field, and to the knock-on effect for research participation and sampling among under-16s

Research Evidence – Children Online

- In July, DSIT published Children's Circumvention Behaviours Online
- Commissioned after the Online Safety Act's child safety duties took effect in July 2025, it examined how children aged 11 to 17 experience age assurance, whether and why they seek to circumvent it, and the role of VPNs
- Some findings include:
    - Nearly 6 in 10 children (58%) have heard of VPNs
    - A quarter (26%) say they have used one in their lifetime and around a fifth (22%) have used one in the last 3 months
    - Lifetime use rises from 17% of 11- to 12-year-olds to 31% of 16- to 17-year-olds
    - Children in London are notably more likely to have used a VPN, with 37% reporting lifetime use — well above the national average
    - A majority (54%) of those who have encountered tick box age checks think they are not effective. For the date of birth check, views are more evenly split — 50% consider it effective and 46% consider it not effective
    - 39% of all 11- to 17-year-olds say they have successfully got around at least one age check - a further 14% have tried without success
    - In total, 53% of children have attempted to bypass an age check at least once

Research Evidence – Children Online

- Methods used by those who have bypassed:
    - Pretending to be someone older — used by 63% of those who have bypassed, equating to 24% of all children
    - The most common specific method is giving a false date of birth (45%)
    - A minority used a parent's or relative's ID (11%), someone else's ID (5%) or altered images or disguises to appear older (6%)
    - Using settings or tools that change apparent location — used by 27% of those who have bypassed, equating to 10% of all children. Among those who used this method and gave an open text response, 60% indicated they had used a VPN
    - Other methods — 22% of those who have bypassed, equating to 8% of all children

- ***Potential impact:*** children taking part in research may be using similar techniques to get around age verification checks

Ofcom Investigation - TikTok

- On 16 July 2026 Ofcom opened an investigation into TikTok's compliance with its duties to protect children under section 12 of the Online Safety Act 2023
- Those duties require providers of regulated user-to-user services likely to be accessed by children to protect them from harmful content, using proportionate systems and processes
- Ofcom states the investigation follows its review of major platforms' child protection measures and its Children's online experiences report, which it says highlighted concerns about children being exposed to harmful content on TikTok
- Ofcom states its Age Assurance report, published the same day, suggests that in some cases age inference models, including those used by TikTok, may have failed to correctly identify a significant proportion of children on their platforms, putting them at risk of exposure to harmful content
- The investigation will seek to establish whether there are reasonable grounds to believe TikTok has failed, or is failing, to comply with these duties, including through its use of age assurance
- The investigation follows Ofcom's review of steps taken by major platforms, its Children's online experiences report, and its Age Assurance report published the same day
- The Age Assurance report examined the effectiveness of age inference models, including those used by TikTok

- ***Potential impact:*** effectiveness of age assurance – not just its presence – is now the regulatory test

ICO Enforcement – Employees

- In 2024, two former RAC employees who had worked as customer service specialists at the RAC's call centre in Stretford were given suspended prison sentences and ordered to complete 150 hours of unpaid work for unlawfully copying and selling over 29,500 lines of personal information
- Their unlawful conduct was discovered by, and reported to the ICO, the RAC after it installed new security monitoring software
- The software showed data had been unlawfully accessed and copied relating to people involved in road traffic accidents
- The information was shared in a WhatsApp chat with a third party who was paying for the information
- In May 2026 the ICO secured successfully outcomes at Proceeds of Crime Act (POCA) hearings
- This resulted in confiscation orders totaling over £118,000 under POCA for the unlawfully copying and selling personal information

Points to Note:

- The outcome of the POCA hearing shows that the ICO will use the full range of its enforcement powers to bring criminals to account and recoup money, calculated by the Court, which reflects the benefit gained from illegal activity
- Two further prosecutions in July 2026 saw council employees given suspended sentences for unlawfully accessing personal records

AI, Confidentiality and Legal Privilege

- In UK and R (Munir) v Secretary of State for the Home Department [2026] UKUT 81 (IAC), the Upper Tribunal considered two immigration cases where advisers filed documents citing cases that did not exist, generated or influenced by AI
- One adviser had also used ChatGPT to summarise official decision letters and redraft client emails by uploading them to the tool
- The Tribunal held that entering confidential material into an open-source AI tool such as ChatGPT places it in the public domain, breaching confidentiality and waiving legal privilege – the first English ruling on the point
- Closed systems operating within a secure network, such as Microsoft Copilot, were distinguished; the Tribunal also referred the representatives to their regulators and stressed verification and supervision

- **Points to Note:**

- The principle is about confidentiality, not lawyers – any organisation loses control of what it uploads to a public AI tool
- For research this covers participant data, client data, briefs, transcripts and unpublished findings, etc.
- Practical steps: use closed or enterprise AI tools, set a written AI policy on what may be uploaded, train and supervise staff, and verify AI output – all these issues are addressed within the MRS AI and Related Technologies guidance

International Update

Debrah Harding

CNIL Fines IQVIA €5m

- On 26 May 2026 the CNIL fined IQVIA Operations France €5 million (SAN-2026-008) over two authorised health data warehouses: LRX, fed by around 14,000 pharmacies, and EMR, fed by several thousand doctors, covering tens of millions of people
- The CNIL acted on complaints following a "Cash Investigation" broadcast, and inspected both the company and partner pharmacies
- It found IQVIA had not respected the terms of its authorisations, in particular on informing individuals, enabling them to exercise their rights, and data security
- Crucially, data that can still be re-identified by the key holder is pseudonymised, not anonymous, and so remains special category health data under Article 9 GDPR
- IQVIA must also bring its processing into compliance within six months, subject to €10,000 per day of delay

- **Points to Note:**

- A landmark on the anonymisation threshold – calling data "anonymised" does not take it outside the GDPR if re-identification remains possible
- Research organisations should revisit anonymisation claims, participant transparency and rights handling across panels and data warehouses

Liability for AI Overviews

- On 28 May 2026 the Landgericht München I (case 26 O 869/26) granted a preliminary injunction against Google – the first German ruling that Google is directly liable for false statements in its AI Overviews
- Two Munich publishing companies sued after the feature wrongly linked them to fraudulent schemes, disreputable business practices and subscription traps
- The court treated Google as a direct tortfeasor: AI Overviews do not merely index and quote sources but generate new, coherent text, so the search engine liability privilege does not apply
- Google's argument that users can check the underlying sources for themselves was rejected, as was the claim that AI-generated statements attract the same free speech protection
- Google faces a penalty of up to €250,000 per breach and is reviewing the decision, which is not yet final

- **Points to Note:**

- A high accuracy rate is no defence – at scale even a small error rate produces millions of wrong answers, and the reputational damage falls on the subject, not the user
- Any organisation publishing AI-generated summaries of others' content should assume it owns those words, and be ready to monitor and correct what its tools say about third parties

Publishers Push Back on AI Scraping

- A coalition of UK news organisations has announced plans to invoice AI companies directly for unauthorised use of their content, and to pursue legal action against those that refuse to pay – a shift from negotiating licences towards billing first and litigating if payment does not follow
- A parallel push is underway in France, where the proposed Darcos Bill would rebalance copyright disputes between creators and AI developers
- The bill tackles the information asymmetry between rights holders and AI providers: instead of the copyright owner having to prove a work was present in training data, it creates a rebuttable presumption of use, shifting the burden onto the AI provider
- It passed the French Senate unanimously in April, but 110 amendments introduced by pro-tech lobbyists in the National Assembly have drawn strong criticism from France's cultural, music and press sectors and pushed the debate back to the autumn

- **Points to Note:**

- A presumption of use would be a significant change – rights holders currently have little practical way of proving their material was ingested
- Research organisations should track how their published outputs are licensed, and contractual terms covering AI training use

AI Search and Referral Traffic

- New analysis from the Danish Media Association and DPCMO examines how AI services are affecting traffic to news and media sites
- Time spent on AI services has risen by more than 600 per cent over a short period, showing how quickly these tools are displacing conventional search behaviour
- Despite that growth, Google AI Mode generated zero referral traffic to Danish media sites over the period analysed
- The finding sharpens publisher concerns: content is being used to answer queries while the traffic, and the advertising and subscription revenue that follows it, does not reach the original source

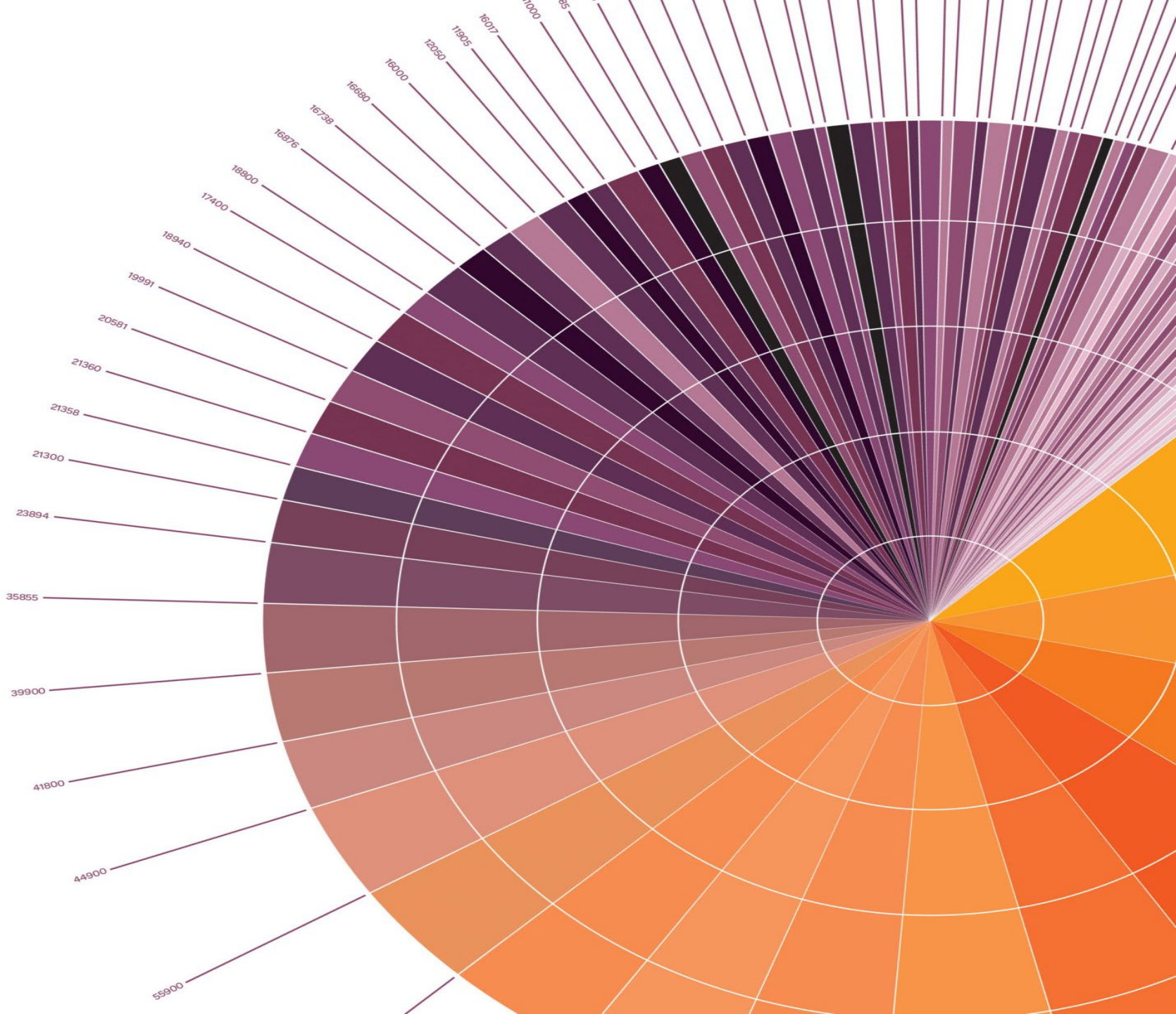
- **Points to Note:**

- This is the commercial argument underpinning the UK invoicing move and the French bill – if AI answers replace visits, licensing income becomes the only route to compensation
- Organisations that rely on web traffic to reach audiences, including for participant recruitment and dissemination of findings, should not assume search referrals will continue at historic levels

MRS Guidance update

Julie Corney

MRS Code of Conduct – 2026/7 revision



MRS Code of Conduct 2026/7 revision

The MRS Code of Conduct revision is ongoing during 2026 on its regular three-year revision cycle.

The Code is crucial in helping to protect and regulate first-rate market and social research, insight and data practice. MRS is committed to keeping the Code under regular review to ensure it is fit for purpose.

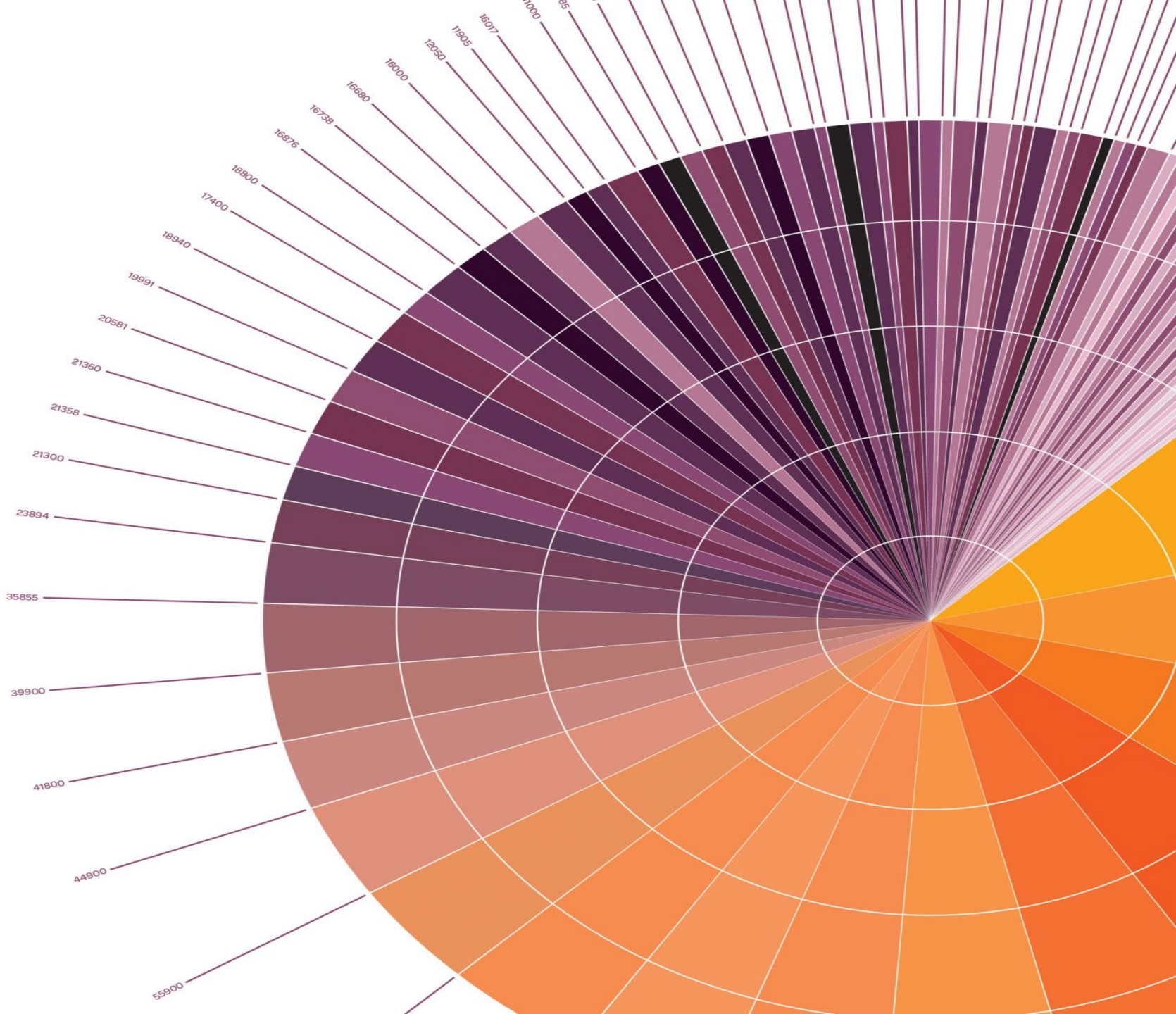
We plan to start the consultation process with the membership late 2026/early 2027.

MRS Code of Conduct 2026/7 revision

Members will have the chance to influence the MRS Code of Conduct revision.

Once the new Code is released, MRS will provide **webinars, briefings, and newsletters** to explain the updates, and there will be a **three-month transition period** from the 2023 Code to the updated version. Members are encouraged to **participate in the consultation** and share any suggestions in advance via **codeline@mrs.org.uk**.

Creating effective complaints procedures



Complaint handling

We expect our members to uphold high standards of professional behaviour and conduct. These standards are set out in the MRS Code of Conduct which every member signs up to when they join MRS.

We take complaints about our members very seriously and we will fully investigate allegations that MRS members have potentially breached our Code.

We have Disciplinary Regulations that set out the processes and procedures that we will follow in taking forward a complaint made about one of our members.

What happens when MRS receives a complaint

The purpose of the MRS Disciplinary Regulations/Company Partner Complaints Procedure is primarily to enforce the provisions of the MRS Code of Conduct and associated regulations and guidance.

If the complaint does not contain allegations that relate to a potential breach of the Code (and/or associated regulations and guidance) then it is likely that the complaint does not fall within MRS's remit to consider.

What happens when MRS receives a complaint

The Standards Department will undertake an initial consideration of any complaint received by MRS to determine whether it reaches the threshold to be referred to the MRSB for formal investigation.

This initial triage stage affords the MRS discretion as to whether to consider complaints that do not meet certain procedural requirements (i.e. complaints that are not made within the required timeframe), are wholly without merit, or that it does not consider to be within its remit. Allowing for complaints to be triaged at this stage means that MRS's resources can be used most effectively.

Introduction

Members and Company Partners must ensure that they do not in any way restrict their ability to comply with the requirements of, and their obligations under, this Code, including co-operating with MRS in any investigations. Members and Company Partners should be particularly mindful of this requirement when entering into contracts, including Non-Disclosure Agreements, with third parties. Failure to do so may be considered to bring discredit on the profession, MRS or its members, in breach of Rule 8 of this Code.

Rule 8 – Members must not act in a way which might bring discredit on the profession, MRS or its Members.

What does this mean for MRS members?

Under the MRS Disciplinary Regulations, membership may be withdrawn or other disciplinary action taken, if a Member is deemed guilty of unprofessional conduct. This is defined as a Member:

…failing without reason to assist the professional body in the investigation of a complaint

What does this mean for MRS Company Partners?

MRS Company Partner organisations are also required, in accordance with the terms of the Service, to take action to ensure that the Code of Conduct is adhered to by all individuals employed or engaged by them (whether MRS Members or not). The rules of this service are detailed in the MRS Company Partner Quality Commitment.

Under the MRS Quality Commitment and its associated Complaints Procedure, MRS Company Partners are committed to comply with the principles and rules of the MRS Code of Conduct and associated Regulations and to co-operate with MRS to assist in the early resolution of any complaints.

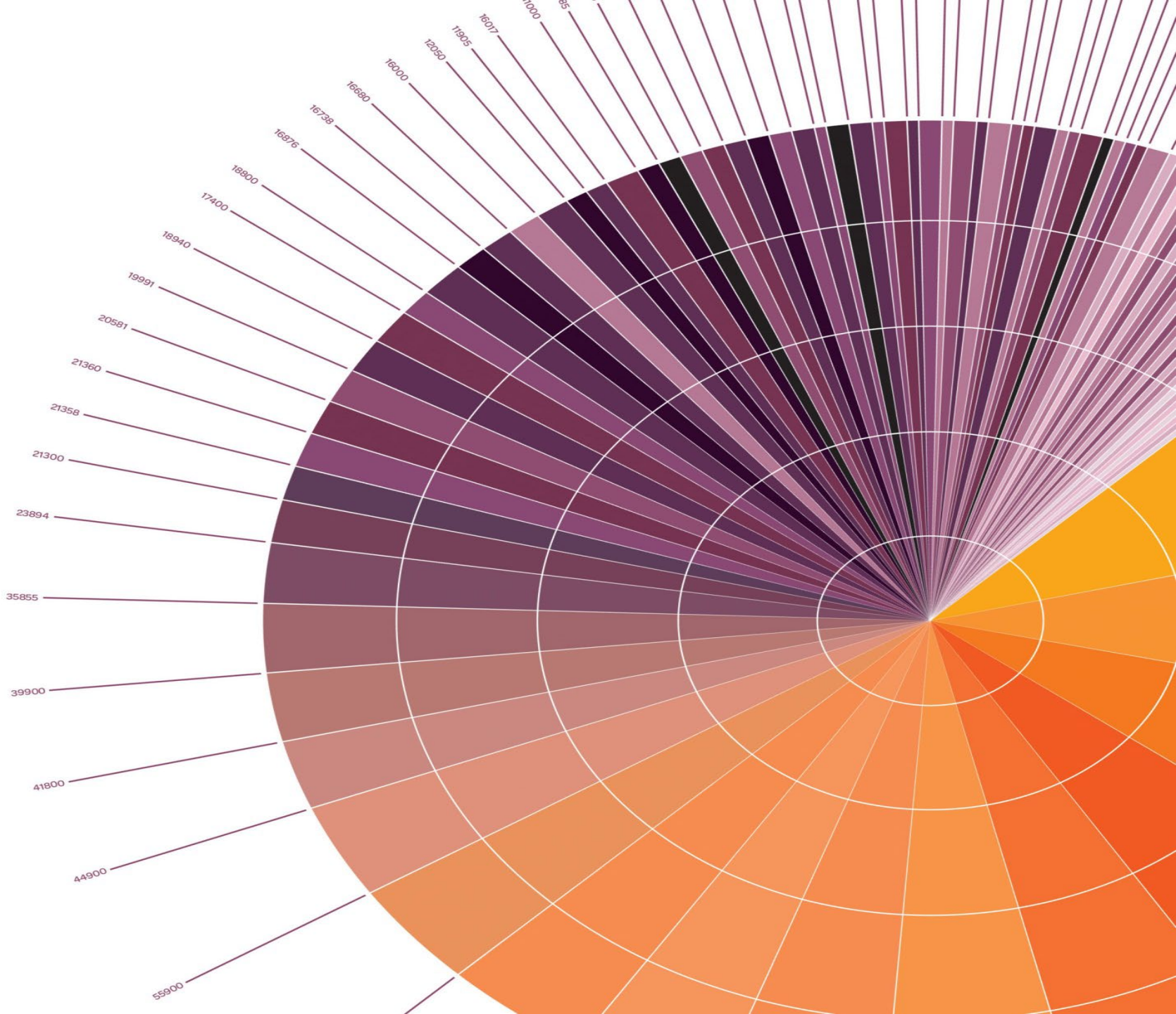
To be Code compliant Members & Company Partners must:

Ensure that contracts with clients/suppliers/third parties/participants do not compromise your adherence to the Code and obligation to assist if a complaint is raised against you

Ensure that Non-Disclosure Agreements adhere to the Code

Ensure co-operation with MRS to assist in the early resolution of any complaints

Vexatious complaints



Vexatious complaints

Complaints should be treated, as a starting point, as having been raised in good faith. Those who complain may well feel wronged or exasperated, or may be driven by other motivations, and this needs to be acknowledged; what matters, however, is a thorough assessment of the substance of the case, not the complainant's manner.

Each complaint requires assessment on its own substance. Where a person has previously raised a vexatious or malicious complaint, no assumption should follow that anything further they submit carries the same character.

Vexatious complaints

Factors to consider in determining whether a complaint may be considered vexatious include (but are not limited to) instances where the complainant:

(a) has explicitly stated, in the complaint itself or in other communications, that they intend to cause disruption;

(b) makes unsubstantiated and serious accusations against members or specific employees;

(c) is from a campaigning organisation, or is someone linked to/representing a campaigning organisation, and their complaint is clearly an attempt to discredit an individual's research without substance or merit;

(d) is targeting a particular member against whom they have some personal grudge;

Vexatious complaints

(e) systematically or frequently sends repeat complaints as part of a campaign with the intention of causing disruption/ waste resources;

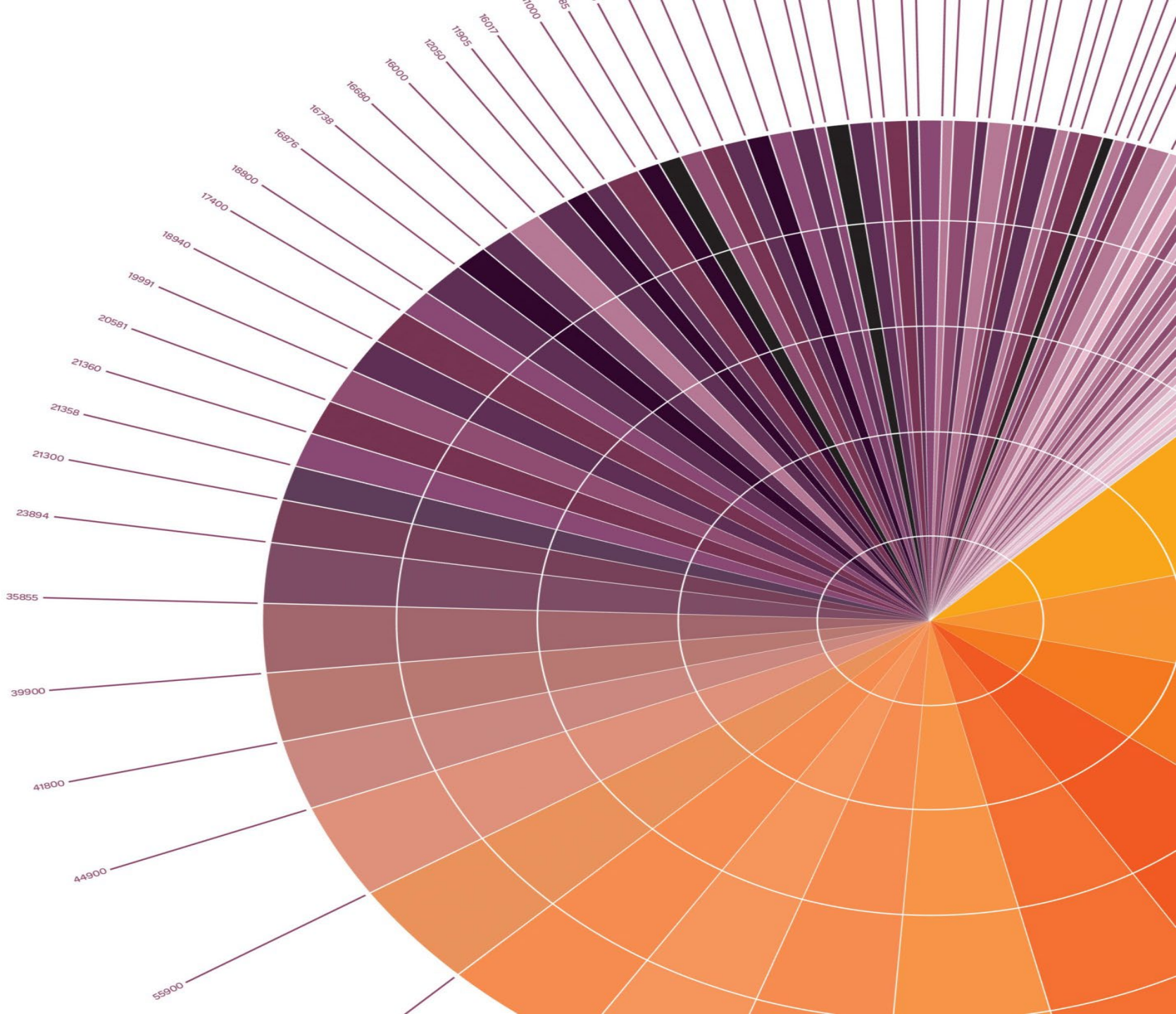
(f) seeks to prolong contact by continually changing the substance of a complaint or by continually raising further concerns or questions whilst the original complaint is being addressed;

(g) fails to clearly identify the substance of their complaint, or the precise issues which may need to be investigated, despite reasonable efforts to assist them;

(h) complains solely about trivial matters to an extent which is out of proportion to their significance;

(i) makes excessive contact with or seeks to impose unreasonable demands or expectations on resources, such as responses being provided more urgently than is reasonable or necessary.

Complaint procedure checklist



Complaint procedure checklist

Prevention is better than cure…

- Setting out how the complaints process works, and staying engaged with those raising them, matters a great deal.
- Put a straightforward complaints-handling procedure in place and ensure it is accessible to all
- Speed of response counts, above all where a complaint appears on social media, since prompt action limits the damage.
- Courtesy and understanding should guide the exchange; resist reacting instinctively or with irritation and give the complainant a proper hearing.

Complaint procedure checklist

- Own the complaint yourself, offering your name as the point of contact, even where colleagues will need to help bring it to a resolution.
- Where social media is involved, a courteous public acknowledgement should be followed immediately by moving the conversation into private channels rather than letting it unfold in the open.
- Keep a record covering the substance of the complaint, the date it was raised, and the complainant’s name and contact details.
- Resolve matters in as timely a manner as possible, wherever that is achievable; failing that, provide the complainant with a realistic time frame for resolution.

Complaint procedure checklist

- Lengthy investigations call for regular progress updates to the complainant
- Unreasonable complaints or demands can be turned down, provided this is done constructively by setting out the resolution you are able to offer.
- Internal steps to stop the issue arising again may also be warranted, whether through staff training or improvements to products, services or systems.

Thank you

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