# Draft Code of Practice on Electronic and Workplace Balloting for Statutory Union Ballots
# Consultation response on behalf of Thompsons Solicitors LLP

Thompsons is the most experienced trade union, employment rights, and personal injury law firm in the country, with 19 offices across the UK. It acts only for trade unions and their members on employment and industrial relations issues.

Thompsons represents most UK trade unions and advises on the full range of employment rights issues through its specialist employment rights department.

Thompsons is a large employer with over 250 employees.

## Overview

Thompsons welcomes the Government's commitment to introducing electronic and workplace balloting for statutory union ballots, but has concerns with the proposals in the Draft Code of Practice on Electronic and Workplace Balloting for Statutory Union Ballots (the "Draft Code"), both as regards specific requirements imposed on unions and scrutineers, and the approach outlined more broadly. Of particular concern is the extent to which the Draft Code appears to "raise the bar" for unions as regards its information management obligations.

Thompsons has significant experience of defending trade unions in industrial action ballot challenges made by employers. It is an unfortunate reality that it is not uncommon for employers to seek to challenge a ballot (often at the last minute after industrial negotiations appear exhausted) on the basis of purported non-compliance with the onerous legislative requirements set by the Trade Union and Labour Relations (Consolidation) Act 1992 ("**TULRCA**"). The most frequently litigated areas of the UK's industrial action legislation are the notification and information provisions. Too often they have been used to create traps and hurdles for trade unions in litigation, which has been the antithesis of good industrial relations.

Whilst there are, of course, instances in which employers may have valid concerns about the integrity of a ballot, in other cases employers seize on purely technical failings to challenge a democratic mandate for industrial action. The Court of Appeal (*RMT v Serco Ltd*; *ASLEF v London & Birmingham Railway* [2011] EWCA Civ 226) has stated TULRCA should not be construed restrictively to enable challenges of this nature to succeed. However, even taking this jurisprudence into account, the provisions remain onerous for unions to comply with. The recent changes introduced by the Employment Rights Act 2025 will assist with changing that position, but we are concerned some of those positive developments in simplifying balloting requirements could be undone if electronic balloting requirements create a new set of traps and hurdles that become a springboard for employer ballot challenges.

Our primary concerns are (1) the extent of record keeping expected to be upheld by unions, (2) the detailed and prescriptive nature of the obligations imposed on unions and scrutineers; and (3) the provision in the Draft Code for ballots to be automatically void where certain conditions arise (e.g., if a ballot database is accessed by a third party). It is important to underline that the European Court of Human Rights has confirmed that strike action is protected by Article 11 of the European Convention on Human Rights (*RMT v UK* Application no. 31045/10 at [84]). Any limitations on the convening and organising of such action (including provisions governing electronic balloting) must not unduly restrict this right.

Whilst we of course acknowledge the aim of ensuring electronic ballots are conducted with sufficient safeguards in place to ensure only those voting are able to vote and there is no third-party interference, we consider this legitimate aim is likely to be better achieved through a Draft Code that imposes minimum standards or principles by which elections are to be conducted, rather than by setting out prescriptive obligations as contained in the current Draft Code, some of which are particularly onerous.

## Terminology

**1. Are there any definitions that are unclear?**

We note that paragraph 17(e)(i) of the Draft Code (definition of Pure e-balloting) does not refer to "virtual internet messaging systems". We consider that this paragraph should expressly refer to virtual internet messaging systems.

We also consider that "virtual internet messaging systems" should not be limited to virtual internet messaging systems associated to an "SMS" number (paragraph 58(c), in order to future proof the Draft Code (as messaging systems are decreasingly connected with SMS numbers). It may also be preferable to replace the term "SMS" with a more generic term to accommodate alternative messaging software (e.g., RCS).

**2. Are there any other terms you would like to see defined?**

We believe that the term "union election ballots" used throughout the Draft Code should be replaced with "statutory union ballots" and that this should be defined by reference to in-scope ballots. This will make clear that the Draft Code does not apply to lower-level union elections (e.g., for local representatives) that do not take place pursuant to statute.

We would also like to see a clear explanation given as to how the existing statutory provisions will fit with e-balloting.

**Responsibilities and requirements**

**3. Is the detail of who the responsible person is for each ballot method clear?**

No, paragraph 23(a) refers to the Responsible Person as being the "General Secretary, or equivalent". The meaning of equivalent is unclear, and the Draft Code should specify whether this means (i) a General Secretary known by a different title; or (ii) the General Secretary plus certain other roles (e.g., President, Executive member). It would also be beneficial to state that the decisions as to appointing and delegating the duties of a Responsible Person must be in accordance with the union's rules.

**4. Are the details of the responsibilities of the Trade Unions clear?**

No. We do not consider it should be considered best practice for unions to check in advance with members that they are willing to receive a ballot other than by post. We consider such a communication is likely to confuse rather than help members, most of whom are likely to use electronic communications far more than postal communication, and may be unaware that ballots delivery methods are currently restricted to post.

We also do not think it should be considered best practice for unions to warn members that if they vote in the presence of their employer they are at risk of inadvertently disclosing their union status and voting decision to unscrupulous employers. In many circumstances, unions would wish to issue such a warning. However, this is highly circumstance dependent, and there may be situations where issuing the warning in these terms could have a chilling effect on participation. Unions should have discretion as to whether and how to issue any such warnings, and it should not be considered a failure to comply with "best practice", if unions decide to give a more nuanced message regarding this. It is of course in unions' interests to protect their members from harm by unscrupulous employers in any event, so they are likely in most scenarios to issue a warning in similar terms to the one proposed.

With respect to the obligations on trade unions at paragraphs 29 (to maintain an up-to-date list of compliant contact methods), and 30(d) (to ensure email addresses, SMS numbers and internet message contact information comply with the Future SI and Code), we refer to our response to question 13, below. For the reasons specified in response to question 13, we do not consider it is appropriate or desirable to restrict sending ballots to workplace contact points, and similarly consider that unions should not be under an absolute obligation to audit and update members' contact details prior to convening an electronic ballot. Please see our response to question 13 where we detail the current position under TULRCA as interpreted by case law, and our specific concerns about introducing these further requirements.

5. **Are there any further responsibilities that should be included for the Trade Unions?**

   No.

6. **Are the details of the responsibilities of the Scrutineers clear?**

   We have no experience of acting as or representing scrutineers, and we therefore do not comment on this question.

7. **Are there any further responsibilities that should be included for Scrutineers?**

   No.

8. **Are the details of the responsibilities of the Employers clear?**

   No. We consider the various recommendations in this section expressed with "should" should be changed to "must". We see no obvious basis for not imposing a complete restriction on the types of behaviours outlined at paragraphs 36 to 38. We further consider the restrictions at paragraph 36 should be expanded to prevent employers from monitoring the electronic ballot process in any way. This restriction should be expressed in broad "catch all" terms to avoid monitoring "in the ordinary course of business" and provide no scope for employers to seek to frustrate the principle of voter privacy. Where such information is logged automatically (e.g., if an employer's systems register each web address visited by an employee), the employer should be restricted from accessing or reviewing this information.

9. **Are there any further responsibilities that should be included for the Employers?**

   Please see our response above. We consider that there should be a clear prohibition on directly or indirectly monitoring voting which is a protected trade union activity under existing legislation.

10. **Are the details of the responsibilities of the Central Arbitration Committee (CAC) clear?**

    Yes.

11. **Are there any further responsibilities that should be included for the Central Arbitration Committee (CAC)?**

    We consider that the CAC should be under an obligation to consult with the union before deciding on a voting method.

**Electronic balloting requirements**

**12. Are the standards required of scrutineers for conducting electronic balloting clear?**

No. Paragraph 49 of the Draft Code states that, in addition to being named in one of the statutory orders referred to in paragraph 47 and having been successfully independently audited against the Cyber Essentials Plus standard ("**CEPS**") (or equivalent), the independent scrutineer "must also be compliant with the other requirements of [Future SI]". These requirements are not described, so there is no clarity what further requirements will be imposed on independent scrutineers.

We further note that the specific controls identified at sub-paragraphs (a) to (e) of paragraph 50 are the same as the requirements contained in the CEPS. As the Draft Code envisages scrutineers will hold either the CEPS or an equivalent, it would seem more appropriate for these controls to be listed as minimum requirements for an alternative to CEPS to be considered as "equivalent", rather than as a list of additional controls on top of the requirement to hold CEPS. Further, we are unsure whether the requirements in sub-paragraphs 50(a)-(e) go beyond what is required for CEPS. We are concerned that including these in the Draft Code could put compliant scrutineers who hold CEPS in breach, e.g., if their systems are securely configured, but they have not removed or disabled every feature, functions, services, or software that could be deemed not "necessary". It is not clear whether a scrutineer would be in breach if they left active on their secure system a feature that made navigating the system significantly easier or more practical, but was not strictly "necessary" to its operation. We consider it would be preferable for the Code to take a less prescriptive approach by requiring scrutineers to meet a minimum establish standard (such as CEPS or equivalent) without specifying the exact approach that the scrutineer must adopt to achieve this. This will reduce the scope for speculative injunction applications to challenge otherwise lawful ballots.

We further note in relation to the requirements at paragraph 51 that many of these duties already exist as a result of the obligations imposed by the UK GDPR. Imposing these additional requirements will create an unnecessary administrative and compliance burden; even if the standard imposed by the Draft Code is no higher than that expected under the UK GDPR, scrutineers will be required to satisfy themselves in relation to each of their in-scope activities that they meet the formulations in the Regulation and the Code. Again, we consider it would be preferable to include less prescriptive detail here, and we consider the legitimate aim of ensuring the integrity of the data and ballot process can be achieved just as well with such an approach.

We are concerned that the requirements as drafted could dramatically increase the cost of compliance for scrutineers, thus increasing costs for unions or reducing the number of scrutineers available.

**13. Are the provisions for distributing pure electronic ballots to eligible voters clear?**

No. We note with concern that paragraph 57 of the Draft Code states that an electronic ballot can only be distributed via a personal (private email address (that must not be an email provided, controlled or accessible by an employer, or a union), an SMS number (that is not an employer-provided number) or a virtual internet message system associated with the same SMS number. We further note with concern the duties imposed on the union and the scrutineer by virtue of paragraphs 59-60 of the Draft Code to review members' information prior to a ballot to remove duplicate or workplace contact details and obtain updated information where these are found.

With respect to the restriction on using employer or union email addresses, unions only hold the contact information provided to them by their members.

Whilst unions typically prefer to communicate with members via channels not controlled by their employer, members sometimes only supply a workplace or union email or work phone number to their union, and unions have limited means to compel members to update their details.

Further, whilst it is, of course, preferable to the union to use communication channels that are not subject to potential monitoring by an employer, we see no basis why it should be a provision of the Draft Code that such channels are not used in any circumstances.

At most, it should be a recommendation in the Draft Code that unions use personal email addresses insofar as is possible in light of the information in their possession.

It is established case law that, whilst unions cannot rely on information they know to be inaccurate, they are not under an obligation to gather more information or otherwise perfect their records before a ballot (*RMT v Serco Ltd; ASLEF v London & Birmingham Railway* [2011] EWCA Civ 226. The provisions of the Draft Code impose significant positive obligation on unions to audit and update their membership information to ensure there are no duplicate or workplace email addresses or SMS numbers (paragraph 59). This is a significant departure from this principle and fundamentally alters the duties on unions as regards information management. Unions take reasonable steps to ensure the information they provide as part of a ballot process is as accurate as reasonably practicable in light of the information in their possession. The construction of paragraph 59 suggests there is an absolute duty on the union to "ensure" there are no duplicate/workplace contact methods. Whilst paragraph 63 suggests that inaccuracies can be remedied by way of reissuing ballots wrongly sent to workplace emails (such that breaches of paragraph 59 would not invalidate a ballot), we nevertheless consider it inappropriate for the Draft Code to fundamentally alter unions' duties in this regard. Whilst we do not consider there should be any bar on using workplace email addresses (in light of the comments in the previous paragraph), if such bar is maintained, we consider that the Code should not introduce an express obligation on unions to "ensure" the removal of workplace

contact details, but that the way in which any ballot inaccuracies ought to be addressed is left to the courts. These onerous requirements are likely to disincentivise unions from using electronic and/or hybrid balloting.

With respect to the restriction on using electronic balloting where union members share an email address (paragraph 58(b)), we are concerned that this disenfranchises union members without a legitimate justification. Of course, such members could still vote by post. However, their right to vote electronically is denied (and their right to vote is therefore interfered with) on the basis they share an email address. In our experience, it is not uncommon for union members, particularly older members or those who are less adept at computing, to share an email address with a spouse or partner. If the union holds the same email address for two members to be balloted in a workplace, we do not see what prejudice is caused by sending two (unique) voting links to that email address.

The requirement at paragraph 62 for the scrutineer to reissue ballots where they receive an email bounce back or SMS delivery failure message also conflicts with the existing law as regards postal ballots, insofar as undelivered ballot papers are not re-sent at present unless information comes to light about a member's new postal address. We consider it would be unduly onerous for unions and scrutineers to be required to monitor undelivered electronic communications and, if a failure to reissue an undelivered ballot could invalidate that ballot, it would be a significant disincentive to electronic balloting. We agree with the TUC that this should simply be a matter of best practice. At most, the union and scrutineer should be required to take all reasonable steps to give all eligible voters the chance to participate, and this duty should not be absolute. If an employee does not reply to communications from the union requesting updated contact information, it may simply be impossible to comply with this requirement.

**14. Are the provisions for distributing hybrid electronic ballots to eligible voters clear?**

Yes.

**15. With respect to electronic balloting, are the requirements for the operation of the virtual ballot clear?**

No. It is unclear how the commissioning party will assure itself that the independent scrutineer meets the prescribed standards. If the commissioning party is under an absolute duty to ensure the scrutineer is compliant with all aspects of the Draft Code, we consider this would be unfeasibly burdensome. We consider that at most the commissioning party should be required to ensure that, at the time the scrutineer is engaged, they hold relevant minimum qualifications/approvals (e.g., CEPS or equivalent).

We note the TUC's comment that it is inappropriate for the state to prescribe that a ballot

must include a spoil option. We share the TUC's concerns that it is inappropriate for the state to manage ballots to this letter of detail, and consider any such requirement should be listed as a matter of best practice at most.

**16. Are the voter platform requirements for electronic balloting clear?**

No. With respect to paragraph 78, we propose "any user" be replaced with "users", such as to ensure that scrutineers cannot be found in breach of the Draft Code where they provide a system that is perceivable, operable, understandable and robust for the reasonable/average user and users with additional needs, but where one user (for reasons not attributable to the scrutineer or for which the scrutineer should otherwise not be held responsible) cannot operate or understand the platform.

In response to paragraph 79, we share the concerns of the TUC that the Draft Code takes an overly prescriptive approach that is likely to result in unnecessary disputes / litigation. It should be a matter for the union and/or scrutineer to decide how best to provide the voting instructions based on the specific facts and circumstances, and we see no basis for imposing the limitations currently drafted, provided the minimum required information is supplied in sufficiently clear language.

With respect to the obligation at paragraph 80 that the voter platform be encrypted to a secure standard that "ensures a level of security appropriate to the risk posed and assures the confidentiality and integrity of the ballot", we consider that the duty to "assure the confidentiality and integrity of the ballot" should not be absolute. It is of course the case that scrutineers ought to take reasonable and appropriate steps in light of the risks posed to ensure confidentiality and integrity. However, we do not consider it will ever be the case that a scrutineer (or any provider of online services) could encrypt information in such a way as to entirely ensure its confidentiality and integrity. Whilst in practice we are confident that the existing draft language would be interpreted in such a way as to give it a workable meaning (i.e., the duty would not be absolute), it would be preferable for the Draft Code to make this clear. An alternative formulation would be "*The voter platform must be encrypted to a secure standard that ensures a level of security appropriate to the risk posed, so as to protect the confidentiality and integrity of the ballot*".

**17. Do you agree that encryption should be to the AES256 standard to ensure the confidentiality and integrity of the ballot?**

We do not express a view on this matter.

**18. Are the Unique Identifying Number requirements clear?**

Yes, subject to our response to question 19.

**19. Are the User Database, and Voter Database requirements clear?**

No. It is unclear whether paragraph 84 is a suggestion as to how scrutineers may wish to organise their data to comply with the requirement to keep user/voter data separate, or is a mandatory requirement and the only way for scrutineers to comply with their obligations. We appreciate there is a need to ensure that it is not possible to identify who has voted and how they have voted, and systems must be designed to ensure this. However, we consider it would be preferable for the Code to set out this restriction without then specifying how it is to be achieved, or making clear that the approach outlined at subparagraphs 84(a) and (b) are suggestions rather than the only compliant approach. Whilst it appears that the most likely compliant approach would be one similar to that outlined in the Draft Code, it is not difficult to envisage a scrutineer having a different way of handling the relevant databases that remains compliant (e.g., a single database with internal restrictions, or additional databases so as to fragment the information further, providing additional security). We do not consider it is desirable for scrutineers to be in breach of the Code where they adopt their own methods to comply with the restrictions and standards imposed, and we consider scrutineers and practitioners are best placed to choose how best to comply. This less prescriptive approach will also accommodate for technological advancement.

**20. Are the provisions for the use of the ballot access method by eligible voters clear?**

Yes. However, we consider that a best practice of two-factor authentication is likely excessive in the circumstances.

**21. Are the Ballot Access Vote Requirements for electronic balloting clear and understandable?**

Yes. However, we are unsure of the reason for the restriction on sending an automated email to voters confirming they have voted.

**22. Are the controls as specified under the heading Database Integrity and Access Controls clear?**

No. We repeat our comments in response to question 16, above, in relation to the obligations imposed by paragraph 97(a) of the Draft Code with respect to "assur[ing] the confidentiality and integrity of the ballot". Namely, we consider that the duty to "assure the confidentiality and integrity of the ballot" should not be absolute. We do not consider it will ever be the case that a scrutineer (or any provider of online services) could encrypt information in such a way as to entirely ensure its confidentiality and integrity. Whilst in practice we are confident that the existing draft language would be interpreted in such a way as to give it a workable

meaning (i.e., the duty would not be absolute), it would be preferable for the Draft Code to make this clear. An alternative formulation would be "Ensure all voter information, the voting platform, votes, user database, voter database, and any relevant information to the conduct of the ballot are encrypted to a secure standard that ensures a level of security appropriate to the risk posed, so as to protect the confidentiality and integrity of the ballot".

With respect to the requirement at paragraph 99 for scrutineer access to relevant databases to be limited to "named individuals", we consider that it would be more practical for the Draft Code to provide for role-based access. This would be more appropriate, as it would enable scrutineers to provide access rights for a defined grouping of its employees, such that information can be accessed when required, regardless of staff absences. Limiting access to named individuals could lead to difficulties if the named individual leaves employment or is otherwise absent. We note that paragraph 100(a) states that role-based access controls must also be in place for the user and voter database in any event. It is not entirely clear how this provision interrelates to the requirements of paragraph 99 as drafted.

**23. Are the requirements regarding the security of the electronic balloting system clear?**

No. It is difficult to envisage an electronic ballot system that is not at least theoretically subject to a risk of single point failure. As drafted, paragraph 104 of the Draft Code appears to imply the scrutineer will be in breach unless it designs a system that is entirely resistant to any single point of failure. Whilst scrutineers can take some steps to minimise risk of single point failure, there are of course risks out of its control or which can be minimised but not removed entirely, such as the risk of server failure. There should not be an absolute duty on scrutineers to design an entirely invulnerable system.

We also have significant concerns about the provisions of paragraph 110(a) that a ballot will be invalidated in the event of any unauthorised access to the voter or user databases. We consider this is a disproportionately rigid rule that will invariably prejudice unions by requiring ballots to be re-run even in circumstances where unauthorised database access has had no or minimal impact on the integrity, security and confidentiality of a ballot. Not only would unions be put to the additional cost of re-running such ballots, it is an industrial reality that participation rates are likely to drop off when ballots are re-run, and members' impression of the union can also be affected. This is therefore not a neutral rule, but one that will prejudice unions. As drafted, the Draft Code draws no distinction between unauthorised access that jeopardises the integrity of the ballot and access that does not, does not accommodate for accidental unauthorised access by an employee of the scrutineer (which would not seem unlikely) or provide for circumstances in which data is accessed by a party for the purpose of frustrating the ballot. Indeed, the current draft effectively incentivises persons hostile to a ballot to seek to access the data, in the knowledge that if they succeed the ballot will be annulled.

**24. Are the requirements regarding the monitoring of the electronic balloting system clear?**

Yes, subject to our comments in question 23 regarding single points of failure.

**25. Are the audit requirements to verify the outcome of the ballot clear?**

Yes. However, paragraph 114 of the Draft Code appears to introduce a method for ballots to be challenged by way of an "audit" of a disputed ballot. This appears to create an additional method for employers to seek to challenge ballots, and may be a significant disincentive in the take-up of electronic balloting by unions, as there is no such equivalent in the context of postal ballots. For postal ballots, employers can of course seek to challenge perceived unlawfulness through litigation. However, employers cannot outside of this sphere compel a union or scrutineer to invite a third party to audit the entire process followed. We anticipate that introducing this power might encourage some unscrupulous employers to dispute ballots (including on speculative bases) in order to delay and/or prevent outright democratically-mandated industrial action.

**26. Do you have any other comments to raise about the Electronic Balloting section of the Code of Practice?**

No.

**<u>Workplace balloting requirements</u>**

**27. Are the standards required of the scrutineers to conduct workplace balloting clear?**

No. We consider that paragraph 131 of the Draft Code should provide that employers are only permitted to refuse a request for a workplace ballot on reasonable grounds. The government may wish to prescribe what would be considered "reasonable grounds" for refusal. As drafted, employers have an absolute veto over workplace ballots, and we consider most employers would rely on this power to refuse requests from unions.

**28. Are the ballot requirements clear?**

No. The "requirements" referred to in paragraph 133 are unclear, and therefore the extent of the obligation on the union to assure itself that the scrutineer meets these is also unclear. These should be specified. Paragraph 137 is vague and we do not see what it materially adds to unions' existing obligations under statute to accord eligible members the right to vote in statutory ballots (see ss 227 and 230(2) TULRCA (we note the latter will need to be amended to provide for electronic balloting)).

Paragraph 136 of the Draft Code cross refers to the section *Responsible Person – Factors and Criteria*. Where the relevant factors and criteria at paragraphs 168 of the Draft Code refer to [Future SI], we cannot comment as to their suitability. We note that one of the factors (at paragraph 168(b)(vi) refers to making contingency arrangements for the conduct of the election in case of a last-minute revocation of the access agreement. We consider it should not be open to employers to revoke access last minute at all.

**29. Are there any further responsibilities that should be included for the parties involved in workplace balloting?**

Please note our comments in response to question 28 generally.

With respect to the minimum requirements of a voluntary access agreement, we do not think that "unreasonable" is a term to be agreed by the parties, and there should simply be a restriction on employers unreasonably withholding staff from voting. Any attempts to define the term will leave open behaviour that falls outside the definition, and it is widely accepted practice in law for "reasonability" to be assessed using its ordinary meaning taking into account the relevant facts and circumstances. We consider the primary risk of workplace balloting is that members' trade union status will be exposed and they may face repercussions or other negative outcomes because their employer has become aware that they have voted. We note that paragraph 143(g) provides that employers must agree not to monitor the balloting location via CCTV or otherwise. We consider that this minimum requirement does not go far enough, and there should be a minimum provision for the ballot to be conducted in such a way that voters can travel to the ballot location, cast their votes and return to work in private without the knowledge of their employer, and a corresponding restriction on employers from seeking to monitor this process at all.

**30. Is there anything else you think the Code should recommend to be included in a voluntary access agreement?**

No. See our response to question 29.

**31. Is there anything else that you think the Code should recommend to be included in the provisions as set out for voter identification?**

We are aware that some union members will not have passports or driving licences. We do not consider it is reasonable for union members to be required to obtain paid ID to exercise their Article 11 rights in a union ballot. We propose that the Future SI or Draft Code should set limits on the powers of scrutineers such that they cannot impose an ID requirement that is limited to passports, driving licences or other forms of paid ID. We consider that the required form of ID should be a matter to be agreed by the parties, and a pay slip might suffice in many instances.

**32. Do you consider this section on the requirements on sites used for workplace balloting clear?**

No. Please note our comments to question 33.

We also consider that the term "suitable" in paragraph 149 should be subject to a reasonability requirement, so that employers do not have an absolute power to veto an offsite work location by claiming that it is unsuitable when this is not in fact the case.

**33. Should the Code include any other recommendations in relation to the requirements set out for each site location to ensure secrecy of the ballot?**

We consider it would be prudent to impose a broader requirement in relation to each type of balloting location that it should be possible for voters to travel to and from the location and exercise their right to vote (or note vote) in private. We note there is already a restriction on active monitoring of the ballot location by CCTV and provision that voting should take place outside the sight of management. However, we consider it would be appropriate to provide further safeguards to ensure members can exercise their right to vote (or not vote) in private. In practice, if members are voting during work hours, they risk exposing their trade union membership status by leaving their workstations to travel to the voting location. We acknowledge it may be impracticable to provide for absolute privacy in this regard, so we propose that this requirement is expressed in similar language to sub paragraph 147(a) (i.e., that voters "should, wherever possible, be able to travel to and from and enter and exit the ballot location out of sight of managers and/or team leaders".

We further consider that, in relation to paragraphs 147(a) and (c) of the Draft Code, which both impose privacy restrictions to be achieved "wherever possible", there should be provision for scenarios where it is not possible to fully meet these requirements. That is, where it is not possible for the location to be out of the direct sight of management or for the ballot location to not be monitored, management should be under a duty not to monitor the location (in relation to subparagraph (a)) and not to review any CCTV/other logs of monitoring (in relation to subparagraph (c)) other than for specified legitimate purposes as agreed between the parties.

**34. Do you have any other comments to raise about the Workplace Balloting section of the Code of Practice?**

No.

**Responsible person**

**35. Are the requirements of the Responsible Person clear?**

No, as these are to be set out in a Future SI, which has not yet been published. Please also note our comments as regards "factors" in question 36. It is unclear what the consequences of non-compliance would be.

**36. Are the factors specified for the responsible person for pure electronic balloting to support decision making when choosing the appropriate ballot method(s) clear?**

No. We consider the requirement to consider "contingency arrangements" would benefit from further guidance or explanation, as it is not clear what level of consideration the Responsible Person is required to give this factor. For example, it is unclear whether they need to reach a fixed conclusion on whether a ballot would be extended in case of an outage. In reality, the answer to this question is likely to turn on the extent and impact of any outage. We note this is a "factor" that should be taken into account (so is not a mandatory criteria), but we are nevertheless concerned about how the imposition of broad, non-mandatory factors for consideration would work in practice, and whether it would be open for employers to challenge a decision to run an electronic ballot on the basis that this factor has not been (sufficiently) considered. If such a requirement is maintained, it should be made clear that the union has discretion to vary any contingency arrangements decided in advance if this is reasonable in the circumstances.

We further consider the Draft Code should provide further details as to circumstances in which scrutineers should block access to the e-balloting platform from certain countries. We note the default position set out in footnote 22 that, by default, best practice is to block all non-UK IP addresses unless otherwise requested. We note that VPN technology makes it possible for people outside the UK to use a UK IP address, such that this factor is unlikely in itself to bolster security. It is also not unlikely that some voters will be abroad at the time of the ballot, particularly in the case of seafarers. Further, we think that such operational matters are best dealt with by the independent scrutineer, who is under a broader obligation to take steps to secure the platform, and that a Responsible Person at a union should not be required to conduct an analysis of the data security specifics as a pre-condition to deciding to conduct an electronic ballot.

We finally note that there is a requirement for Responsible Persons to consider as a factor whether electronic balloting is "secure". We think this term could benefit from guidance or definition. There will of course be security risks with any method adopted, and it will be difficult for Responsible Persons to satisfy themselves they have complied with their duty under paragraph 166(a)(i) without some limits on the term "secure".

**37. Do you think the Criteria specified for the responsible person for pure electronic balloting are clear?**

No. Please note our comments elsewhere in this consultation response as to our concerns about restrictions on using non-personal email addresses, and the higher standards imposed by the Code in relation to e-ballots as compared to established case law on postal ballots. We do not consider it is appropriate or feasible for a Responsible Person to be required to conclude as a pre-condition of deciding to run an e-ballot that the method adopted will "ensure" that everyone eligible to vote receives the opportunity to do so, that all email addresses/SMS numbers are "personal" (paragraphs 166(b)(iii)-(iv)). Whilst best endeavours can be used to audit this information, this requirement imposes a significant administrative burden on the union and, as unions are reliant on the information they are provided by members, it would be difficult to guarantee these requirements have been complied with in their entirety, particularly at such an early stage in the process.

**38. Are the Factors specified for the responsible person for hybrid electronic balloting to support decision making when choosing the appropriate ballot method(s) clear?**

Please see our response to question 37.

**39. Do you consider the Criteria specified for the responsible person for hybrid electronic balloting are clear?**

Please see our response to question 38.

**<u>Workplace Balloting</u>**

**40. Are the Factors specified for the responsible person for workplace balloting to support decision making when choosing the appropriate ballot method(s) clear?**

Please see our response to question 37. We consider the Draft Code would benefit from some guidance or further comment as to what is meant by "appropriate" in the context of paragraph 168(a)(i), so that Responsible Persons can better understand the factors they must consider.

**41. Do you consider the Criteria specified for the responsible person for workplace balloting are clear?**

Please see our response to question 38.

**42. Do you have any other comments to raise about the Responsible Person section of the Code of Practice?**

No.

**Compliance and enforcement**

**43. Are the additional scrutineer reporting requirements clear?**

Yes.

**44. Do you think the Code should include any other recommendations with respect to the additional requirements in scrutineer reports for ballots conducted with the new permitted methods?**

No.

**45. Are there any areas in the Code of Practice that you think would benefit from further guidance?**

No, subject to our comments elsewhere in this response.

**46. Do you have any comments on the overall structure of the Code?**

No, subject to our comments elsewhere in this response.

**Thompsons Solicitors LLP**
**28 January 2026**