



Information Commissioner's Office
Promoting public access to official information
and protecting your personal information

THE CO-ORDINATED ONLINE RECORD OF ELECTORS (CORE) CONSULTATION PAPER

Q1: Do you agree that Models 4 and 5 are best suited to meet the aims and objectives of Phase 2 of the CORE project? If you disagree, please state which model you believe would be a better fit and set out your reasons.

In terms of delivering a solution which meets the required functionality in order to meet the stated objectives, Models 4, 5 and 6 seem to be most appropriate. As these also present the lowest risk and risk takes into account both technological and security failure, from a data protection perspective these seem like the best models to use.

Q2: Do you agree that all information that currently appears on the full register of electors should be held in the CORE? If you disagree, please state which information from the full register you believe should NOT be held in CORE, and set out your reasons.

The CORE system should contain only the information necessary for its effective use, i.e. to meet the stated aims and objectives of such a system. As these stated aims include improving the integrity of electoral registers, providing more efficient access to the data and improvements in the electoral administration process it would probably be necessary to hold all information currently appearing on the full register of electors in CORE.

Access should be controlled to ensure that current access levels are maintained and that nobody gains access to information which they currently cannot see. Also, whilst this information is currently publicly available, there are particular constraints on how people view it and for what purposes – holding the information centrally in an electronic format means that people potentially have more ready access to information about all those registered to vote and the security of such a system to ensure that breaches are not made and to ensure current access levels are maintained is extremely important.

Q3: If responsibility for retention of the marked register is in future to be the responsibility of EROs, what is your estimate of the cost of getting such information imported to a consolidated CORE system? Do you think good value for money and benefits to the integrity of the election would result?

N/A – this is not an area we can comment on.

Q4: Do you agree that information set out in the statutory absent voter lists maintained by EROs should be supplied to a consolidated CORE system? If you disagree, please set out your reasons.

If this information will have a purpose in meeting the aims and objectives in using CORE and will therefore be necessary for its proper functioning then it may be necessary to include it in the CORE system. However, it would be important to ensure that only those currently authorised to have access to this information have access within CORE. It is also important not to include this information purely on the basis that it may become useful in future, a decision must be made based on current plans for implementation of the system.

Q5: Do you agree that any additional personal identifier information on individuals that is gathered during electoral registration should be supplied to a consolidated CORE system? If you disagree, please set out your reasons. Views on what types of personal identifier might be particularly useful and realistic for use in a CORE context would also be welcomed.

As above, if this information is necessary in order for the CORE system to fulfil its stated purpose and is necessary for the EROs to continue to carry out their functions then it can be stored within CORE. However, (and as also stated previously), the potential for the information to be accessed unlawfully due to it being held on a centralised electronic system means that security levels and access controls will need to be suitably stringent to safeguard against any misuse of the information.

The types of personal identifier to be used should also be adequate for their purpose. If the idea is to accurately identify an individual and thus improve the integrity of the register using a date of birth and a signature may not be sufficient, particularly as the date of birth of an individual is quite widely available.

Q6: Do you agree that any future anonymous elector details should be supplied to a consolidated CORE system, subject to the same restrictions on access as apply to the originating ERO? If you disagree, please set out your reasons.

This is a sensitive area as presumably people who request to register anonymously have very pressing reasons for doing so, e.g. to ensure their personal safety. Would it be entirely necessary to the proper functioning of the CORE system to hold information on anonymous voters in the centralised system, taking into account the added risks this poses in terms of unauthorised access and what the risk of harm may then be to these individuals? If it is necessary for integrity checking for example, consideration should be given to identifying a privacy friendly way of holding this information that would still allow this. Similarly privacy enhancing technologies should be explored to ensure adequate protection for this type of information.

Q7: Do you agree that the Government should make use of EML-compliant software mandatory on EROs by the end of 2006 to enable complete UK coverage of CORE Phase 1 electoral registration software standardisation? If you disagree, please set out your reasons.

N/A – this is not an area we can comment on.

Q8: Do you agree that the Government should actively pursue the possibility of using the Government Connect network for CORE data transactions, whilst also – for the time being – exploring the viability of alternative networking approaches? If you disagree, please set out your reasons and what approach to establishing a suitable network you would prefer.

As the Government Connect network provides the opportunity to make use of a system which has been set up to specifically address issues of data transfers and electronic working for government bodies it would appear to be a good network to use for the CORE project. If, however, this network will not be ready in time for CORE, it would also be advisable to continue to look into the viability of alternative approaches.

Q9: Do you agree that EROs should send updates to a CORE central system on a daily basis? If you disagree, please set out your reasons and what frequency of updating you would prefer to see instead.

The Data Protection Act 1998 requires that personal data is accurate and up to date, therefore the more frequently the system can be updated to reflect any changes the better in terms of accuracy. It is unclear from paragraphs 48-54 of your paper whether the five-day period to allow for objections would confuse matters if the register were updated on a daily basis. Presumably the system would be able to deal with any updates where an objection is subsequently raised and therefore the updated information is removed?

Q10: Do you agree that data sent by EROs should go straight into the CORE record, with subsequent integrity checking and reporting of possible anomalies? If you disagree, please set out your reasons.

This method of updating the CORE would seem to retain control of the information and any decision-making associated with that with the EROs and this is in keeping with the current system. In order to keep this version accurate however it would be important that any anomalies were reported promptly and acted on promptly by the ERO given that the 'live' system would show the information as fully accepted.

Q11: Do you agree that, in areas where a CORE scheme is operational, specified large-scale users of electoral registration data should no longer be able to obtain such data direct from local EROs? If you disagree, please set out your reasons.

In terms of data protection the issue in this case is not where these large-scale users get the information from but what information they get. If they are to go straight to CORE rather than to local EROs as they have done traditionally, safeguards must be in place to ensure that they are not gaining access to any information which previously was unavailable to them and which is not set out in the regulations. As an aside, this also raises the issue that, if the CORE keeper is to respond to requests for this information, they become a data controller in their own right where previously the EROs have been data controllers for this information.

Q12: Do you think that, in areas where a CORE scheme is operational, smaller-scale users of electoral registration data should: a) only be able to obtain copies of the information from CORE; b) have the option to obtain the copies either from their local ERO or CORE; or c) only be able to obtain the copies from the local ERO? Please set out your reasons.

As above, the issue in terms of data protection in this context centres around ensuring that people only gain access to the information they are entitled to see. As mentioned in paragraph 65 of your paper, there is already some confusion amongst EROs around whether or not an organisation is entitled to the full or the edited register and adding in an additional body to provide access may complicate this further. We think it would be a good idea for one body to provide access, for both large-scale and small-scale users but given some of the current issues highlighted in the paper, there should be clear and helpful guidelines produced for that body to help it determine when it can and when it cannot provide the requested information.

Q13: Do you agree with the proposal that returning officers should continue to obtain the register and other information required to conduct the election direct from the relevant EROs, rather than from CORE? If you disagree, please set out your reasons.

If the register maintained by the local ERO remains the legal register as opposed to the CORE version and is the one which is most accurate at any given time then it is important that returning officers use this version to gain elector information for running an election. However, this also has implications for the other users of the register as mentioned in questions 11 and 12 as they too should have access to the most accurate and up to date version.

Q14: Do you agree with the proposal that a CORE keeper should not be subject to the requirements for making a copy of the full register available for personal public inspection? If you disagree, please set out your reasons.

As the system currently stands an individual can go and inspect their entry, and where relevant another's, on the register maintained by their local ERO and we do not see any need to change this provision.

Q15: Do you agree with the proposal that authorised bodies should be granted direct electronic access to the CORE central dataset to browse

and/or initiate an electronic search for an individual record? If yes, we would welcome your views on how a charging structure might work for those who are normally expected to pay for copies of the register. If you disagree, please set out your reasons.

There is an argument that by requiring authorised bodies to log in to CORE and perform a search under controlled access conditions you are actually providing more refined access to the pertinent information rather than supplying the full register as currently happens. As you state in paragraph 77 the controls which currently apply on data from the full register and its uses must continue to apply and you would need to take into account security/access controls to adequately ensure that the information being viewed is being used for the lawful purposes.

It is inappropriate for us to comment on a suitable charging structure for those normally expected to pay for a copy of the register.

Q16: If direct access to a CORE system for the purpose of confirming identity were to be established, we welcome views on who exactly should be given the ability to use that facility.

In response to this question and question 15 above, it should be remembered that the more organisations/people you provide with direct access to CORE the more potential for security breaches occur as well as the possible misuse of information. Direct access takes control away from the ERO in determining who should see what information and it would require the CORE keeper to effectively manage this access instead.

One of the aims of setting up CORE is to provide more efficient access to registration data for those authorised but this should be weighed against the possible risks to individuals in terms of misuse of data by providing direct access to a centralised system and the logistics of managing this effectively.

Q17: Do you agree with the proposal that online/telephone access to CORE should be made available for householders to confirm the accuracy of a pre-completed canvass form (for forwarding to the relevant ERO), but not to make changes (including adding or deleting electors)? If you disagree, please set out your reasons.

As far as this reflects what is currently happening (Paragraph 83) we cannot see any major issues with this. However, as stated in previous correspondence, in order to improve the integrity of the system, using such a service would be preferable with individual registration forms rather than household ones.

There would also need to be appropriate security measures to safeguard against abuse of this process.

Q18: Do you agree with the proposal that an individual elector should be able to access directly all the information held on them by a CORE

system, for the purpose of confirming accuracy and/or requesting changes? If you agree, please state whether you would prefer to see the ability to confirm accuracy and request changes implemented at the same time or the ability to request changes implemented later. If you disagree, please set out your responses.

We have stated in previous correspondence that we prefer a system of individual registration and certainly would prefer individual access to alter details online than head of household access. As also mentioned previously in this paper, security is paramount in this situation. Firstly, there needs to be a way of checking that the person logging on claiming to be 'John Smith' really is that person before they are given access to John's details within CORE. If household registration forms continue being used and you are relying on a form of unique log-in detail on that form (as mentioned in paragraph 83) we would be concerned that this potentially gives access to all individuals within one address. This is especially important given your proposal to not only make the full register details available but also any absent voting preferences, marked register information, anonymous elector details and personal identifiers.

Q19: Do you agree with the proposal that CORE should look to use the Government Gateway and/or Government Connect 'Register' strand as the means by which an individual may verify themselves and gain direct online access to the information held about them on CORE? If you disagree, please set out your reasons.

As mentioned above, the ability to correctly identify that an individual is who they say they are when they wish to log on to CORE to make changes to their details is very important. Insofar as the Government Gateway/Government Connect 'Register' has been specifically developed to provide secure access to government services it would seem that this is an appropriate mechanism for verification. Our understanding is that there are different levels of security specified within the Gateway and, given the nature of the information which would be available via CORE (particularly any anonymous elector details), high levels should apply.

Q20: Do you agree with the proposal that CORE should cross-match information it holds, to identify apparent multiple instances of the same individual elector? If you disagree, please set out your reasons.

As one of the stated aims and objectives of CORE is to improve the integrity of the electoral register and the centralised database has been set up for this amongst other purposes, it would seem odd for it not to cross-match the information it holds in order to identify apparent multiple instances of the same individual elector.

Q21: Do you agree with the proposal that CORE should cross-match information it holds, to identify apparent instances of the same individual acting as proxy for more than two electors? If you disagree, please set out your reasons.

See answer to Q20 above.

Q22: Do you agree with the proposal that CORE should cross-match information it holds, to identify apparent instances of the same address being used as the mailing address for the postal votes of multiple electors? If you agree, what do you think might be an appropriate threshold figure at which an alert should be triggered? If you disagree, please set out your reasons.

See answer to Q20 above.

We are not in a position to suggest an appropriate threshold at which an alert should be triggered.

Q23: Do you agree with the proposal that CORE should cross-match information it holds, to identify apparently inappropriate instances of multiple voting by the same individual? If you disagree, please set out your reasons.

See answer to Q20 above (where it is deemed appropriate that CORE should contain additional information such as marked registers).

Q24: Do you agree with the proposal that CORE should refer apparently anomalous information it receives back to the original EROs? If you disagree, please set out your reasons.

Please see answer to Q10 above. This option seems to retain control of the information input into CORE with the relevant ERO and is therefore more in keeping with the current system.

Q25: Do you agree with the proposal that an ERO should be required to actively respond to formal notifications from CORE of apparent anomalies? If you disagree, please set out your reasons. Whether you agree or disagree, we would welcome any informed assessment of what the initial and longer term resource impact of any such requirement would be on EROs.

Requiring the ERO to actively respond to CORE when an anomaly is notified would seem to be a good way of managing the process and ensuring that no notifications are forgotten about and that there is no confusion about whether or not an anomaly is real. It would also provide an audit trail of decisions taken.

It would be difficult for us to make an informed assessment of what the initial and longer term resource impact would be on EROs but presumably this is an inevitable effect of attempting to improve the integrity of the register.

Q26: If a requirement to respond is established, we welcome views on how frequently such notifications should be sent, how long an ERO

should have to respond, and what penalty (if any) should attach to any failure to respond.

The Data Protection Act requires that information is accurate and up to date. Taking into account proposals earlier in this consultation paper to provide access to third parties to the CORE register it would seem to be important that any notifications be sent frequently and be dealt with frequently by the ERO, otherwise the information being provided to third parties may be inaccurate. Whilst the CORE itself provides the mechanism for identifying anomalous entries, for the integrity of the register to actually be improved it requires the input of the ERO in terms of making timely investigations of any possible anomalous data.

The actual frequency may rely on how frequently the ERO ends up updating the register (as asked in a previous question). This would then inform how often the CORE does a search for anomalous information.

Q27: Do you agree with the proposal that an ERO should be able to run a check online with CORE to see whether a particular individual already has a record held on that dataset? If you disagree, please set out your reasons.

As stated in previous responses, this sort of function seems to be in keeping with the aims and objectives of setting up CORE, i.e. to improve the integrity of the register. Using a search function would be preferable, whereby the ERO can input the details they hold on an elector and instigate a search of CORE to find any matching details.

Q28: Do you agree with the proposal that CORE should be able to provide statistical data? If you disagree, please set out your reasons.

Provided that the information were anonymised there would not be any data protection implications with doing this.

Q29: Do you agree with the proposal that CORE should, once established, discharge the statutory mutual reporting responsibilities concerning EU citizens voting in European Parliament elections? If you disagree, please set out your reasons.

In terms of simplifying the process currently used whereby information received from other member states is distributed to relevant EROs via a government department this suggestion seems valid. However, given the comment in an earlier section of the consultation paper which suggested that ERO registers should continue to be used for returning officers as they would be the most accurate and up to date, it is hard to justify how the CORE record could then be used in this context.

Q30: Do you think CORE Phase 2 should be established in geographical stages, or to cover the whole UK at once? If in stages, please state what level of geographical coverage you believe would be appropriate for the

first CORE scheme. Suggestions as to which particular area(s) should be part of the first scheme and expressions of interest would be particularly welcome.

N/A – this is not something we are in a position to comment on.

Q31: Do you think that the Electoral Commission should be appointed as the keeper of a CORE scheme? If you do, would your answer differ if a first scheme was on a relatively small scale? If you would prefer to see some other body appointed as CORE keeper, please say who and set out your reasons.

It is difficult for us to say who would be best placed to act as keeper of the CORE scheme, whether on a large or small scale. In terms of the Electoral Commission's current role however, they would seem to be well placed to be considered as a potential candidate.

Q32: Do you think any of these potential future linkages of an electoral registration dataset with other datasets should be explored more actively in future? Please set out the reasons why you think they should or should not be further explored, and detail which datasets may be more suitable for CORE to link to if there were to be such linkage in the future.

We recognise that in order to improve the integrity of the register data matching exercises with other databases may be desirable and we prefer the use of other public sector databases rather than any private sector ones to ensure greater coverage of the population and to limit intrusion into the lives of individuals in non public sector activities. In paragraph 137 you mention the fact that the nature of the information held in some other databases may mean that there is no value in linking to them and this is important in data protection terms. The information you link to must be useful for your purposes, it should be sufficient and relevant but not excessive. Lots of databases to which you could link will hold information which is useful to you as well as further information specific to the particular purpose of that database. You would need to consider from the outset what information you actually need access to and limit your access to that information alone.

We are not in a position to say which databases would be most suitable for your purpose but hope that the above will be of use when you are making a decision.