Bolton Clinical Commissioning Group

Data Privacy Impact Assessment Procedure and Proforma

Policy Number	**IG011**
Target Audience	**CCG/GMSS Staff**
Approving Committee	**CCG Chief Officer**
Date Approved	**May 2018**
Last Review Date	**May 2018**
Next Review Date	**May 2020**
Policy Author	**GMSS IG Team**
Version Number	**V5.0**

The CCG is committed to an environment that promotes equality, embraces diversity and respects human rights both within our workforce and in service delivery. This document should be implemented with due regard to this commitment.

This document can only be considered valid when viewed via the CCG's intranet. If this document is printed into hard copy or saved to another location, you must check that the version number on your copy matches that of the one online.

Approved documents are valid for use after their approval date and remain in force beyond any expiry of their review date until a new version is available.

Version Control Sheet

Version	Date	Reviewed By	Comment
0.1	September 2013	M Robinson D Sankey	Progress to CCG Executive for approval
1	September 2013	CCG Exec	Approved
1.1	July 2015	IG Team	Organisation change to GMSS and rebranding of PIA to BCCG
1.2	July 2016	IG Team	No substantial changes. Review for Approval
2.0	August 2015	IM&T Operations Board	Approved
3.0	April 2018	IG Team	Reviewed in line with GDPR
4.0	May 2018	IM&T Operations Board	Approved
5.0	May 2018	CCG Chief Officer	Approved.

Analysis of Effect completed:	By: M Robinson	Date: September 2013

Why do I need to complete a Data Privacy Impact Assessment?

Data Protection Impact Assessments (DPIAs) help organisations identify, assess and mitigate or minimise privacy risks with data processing activities. They're particularly relevant when a new data processing process, system or technology is being introduced.

DPIAs also support the accountability principle, as they help organisations comply with the requirements of the General Data Protection Regulation (GDPR) and demonstrate that appropriate measures have been taken to ensure compliance.

A DPIA is a proforma or risk assessment which asks questions about the process or new system based on data quality / data protection / information security and technology.

When do I complete a Data Protection Impact Assessment?

If you are doing any of the following:

- setting up a new process using personal confidential data (PCD)
- changing an existing process which changes the way personal confidential data is used
- procuring a new information system which holds personal confidential data

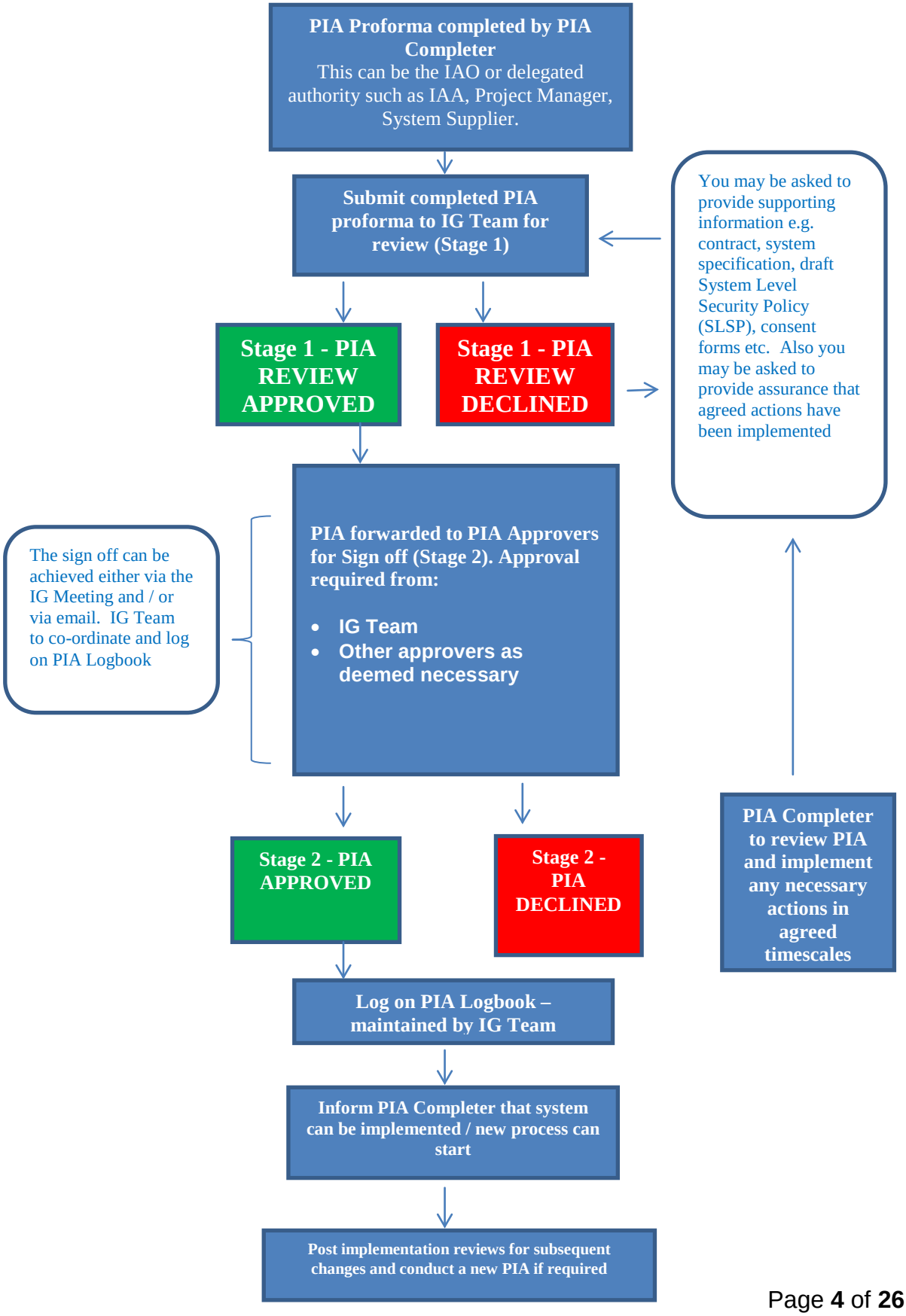
They must be completed as early as possible to ensure risks can be identified and mitigated to an acceptable level.

Who needs to complete a Data Privacy Impact Assessment (DPIA)?

It is the Information Asset Owners / Administrators responsibility to ensure this is completed and submitted. They can delegate this task to an Information Asset Administrator (IAA) / Project Manager and or suppliers of a system / asset.

PIA Process Flowchart

The following flowchart highlights the steps once the PIA has been completed until either approval and / or rejection decision has been reached.



Important

By completing this Data Privacy Impact Assessment, you agree to adhere to the IG Toolkit requirements and have Information Governance and Information Security Policies in place which includes:

- Information Governance Policy
- Completion of Information Governance Mandatory Training
- Information Governance Incident Reporting Procedures
- Secure Transfers of Information Procedure
- Information Asset Register

The list above is not exhaustive.

In the event of an incident and failure to have the above may incur to a larger monetary penalty being levied upon you by the Information Commissioners Office (ICO).

Help and Advice

For further help and advice, please contact the Senior IG Officer for your CCG.

Screen 1: Basic Information

Reference: 00
PIA Title:

PIA Completer Name: *(please note this can be Project Manager / IAO / IAA or whoever has been requested to complete the proforma):*	
Department:	
Email:	
Telephone No.:	
New System / Process Name:	
New System Supplier Name: (if applicable):	
Date System due to go live (if applicable):	
Project Proposal / Purpose for completing PIA:	
Link to wider initiative *(if applicable)***:**	

<table>
<tr><td>Information Technology Involvement</td><td>List any applicable electronic systems/software to this initiative (current and/or new):
<table><tr><th>System name</th><th>Used by e.g. organisation and dept.</th><th>Parties/system supplier</th></tr><tr><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td></tr></table></td></tr>
<tr><td>Are any other organisations are involved in this initiative?</td><td></td></tr>
<tr><td>Confirm all relevant organisations have or are working towards cyber essentials</td><td><table><tr><th>Organisation/Parties/ system supplier</th><th>Cyber essentials Y/N
Working towards/cyber compliance defined under terms of contract</th></tr><tr><td></td><td></td></tr><tr><td></td><td></td></tr><tr><td></td><td></td></tr><tr><td></td><td></td></tr><tr><td></td><td></td></tr></table></td></tr>
<tr><td>Is this initiative in line with or achieving national or local guidance/
strategy or mandate?</td><td>If yes give details</td></tr>
</table>

Screen 2: Screening Questions

Documenting here which of the screening questions are applicable to your initiative will help to draw out the particular privacy considerations that will help formulate your risk register later in the template

		Yes	No	Unsure	**Comments** *Document initial comments on the issue and the privacy impacts or clarification why it is not an issue*
a)	Is the information about individuals likely to raise privacy concerns or expectations e.g. health records, criminal records or other information people would consider particularly private?	☐	☐	☐	Click here to enter text.
b)	Will the initiative involve the collection of new information about individuals?	☐	☐	☐	Click here to enter text.
c)	Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	☐	☐	☐	Click here to enter text.
d)	Will the initiative require you to contact individuals in ways which they may find intrusive[1]?	☐	☐	☐	Click here to enter text.
e)	Will the information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	☐	☐	☐	Click here to enter text.
f)	Does the initiative involve you using new technology which might be perceived as being intrusive? e.g. biometrics or facial recognition	☐	☐	☐	Click here to enter text.
g)	Will the initiative result in you making decisions or taking action against individuals in ways which can have a significant impact on them?	☐	☐	☐	Click here to enter text.
h)	Will the initiative compel individuals to provide information about themselves?	☐	☐	☐	Click here to enter text.

If you answered **YES or UNSURE** to any of the above you need to continue with the Privacy Impact Assessment.

***Sign off if no requirement to continue with Privacy Impact Assessment*:**	
Confirmation that the responses to a – h above is NO and therefore there is no requirement to continue with the Privacy Impact Assessment	
Agreed by:	Click here to enter name of group or individual(s).

Screen 3: Contact Information

Project Management Details	
Project Manager:	
Project Manager Email:	
Project Manager Telephone No.:	
Information Asset Owner (IAO) Details	
IAO Name:	
IAO Title:	
IAO Department:	
IAO Email:	
IAO Telephone Number:	
Information Asset Administrator (IAA) Details	
IAA Name:	
IAA Title:	
IAA Department:	
IAA Email:	
IAA Telephone Number:	

Screen 4: Personal Confidential Data Items

What data items are being processed e.g. for collection, storage, use and deletion: If there is a chart or diagram to explain please attach as an appendix			
Data Item	**Description**	**Specific data item(s)**	**Justification** Reason that the data items(s) are needed – this must stand up to scrutiny for Caldicott justification
Personal Details	Information that identifies the individual and their personal characteristics	Check all that apply: ☐ Forename(s) ☐ Surname ☐ Address ☐ Postcode ☐ Date of Birth ☐ Age ☐ Gender ☐ Physical description ☐ Home Telephone Number ☐ Mobile Telephone Number ☐ Other Contact Number ☐ Email address ☐ GP Name and Address ☐ Legal Representative Name (Next of Kin) ☐ NHS Number ☐ National Insurance Number ☐ Photographs/Pictures of persons ☐ Other – if this is ticked please list 'Other' personal data items to be processed below: See attached	Click here to enter text.

What data items are being processed e.g. for collection, storage, use and deletion: If there is a chart or diagram to explain please attach as an appendix			
Data Item	**Description**	**Specific data item(s)**	**Justification** Reason that the data items(s) are needed – this must stand up to scrutiny for Caldicott justification
Physical or Mental Health or Condition	Information relating to the individuals physical or mental health or condition. NB. For mental health this would include the mental health status i.e. whether detained or voluntary under the Mental Health Act.	☐ Yes ☐ No ☐ Not applicable List any data items below or attach as an appendix: Click here to enter text.	Click here to enter text.
Sexual Identity and Life	Information relating to the individuals sexual life	☐ Yes ☐ No ☐ Not applicable List any data items below or attach as an appendix: Click here to enter text.	Click here to enter text.
Family Lifestyle and Social Circumstances	Information relating to the family of the individual and the individuals lifestyle and social circumstances	☐ Marital/partnership status ☐ Carers/relatives ☐ Children/dependents ☐ Social status e.g. housing ☐ Not applicable ☐ Other - please specify below: Click here to enter text.	Click here to enter text.

What data items are being processed e.g. for collection, storage, use and deletion: If there is a chart or diagram to explain please attach as an appendix			
Data Item	**Description**	**Specific data item(s)**	**Justification** Reason that the data items(s) are needed – this must stand up to scrutiny for Caldicott justification
Offences including Alleged Offences	Information relating to any offences committed or alleged to have been committed by the individual	☐ Yes ☐ No ☐ Not applicable List any data items below or attach as an appendix: Click here to enter text.	Click here to enter text.
Criminal Proceedings, Outcomes and sentences	Information relating to criminal proceedings outcomes and sentences regarding the individual	☐ Yes ☐ No ☐ Not applicable List any data items below or attach as an appendix: Click here to enter text.	Click here to enter text.
Education and training details	Information which relates to the education and any professional training of the individual	☐ Education/training ☐ Qualifications ☐ Professional training ☐ Not applicable ☐ Other - please specify below: Click here to enter text.	Click here to enter text.

What data items are being processed e.g. for collection, storage, use and deletion: If there is a chart or diagram to explain please attach as an appendix			
Data Item	**Description**	**Specific data item(s)**	**Justification** Reason that the data items(s) are needed – this must stand up to scrutiny for Caldicott justification
Employment details	Employment and career history	☐ Employment status ☐ Career details ☐ Not applicable ☐ Other - please specify below: Click here to enter text.	Click here to enter text.
Financial details	Information relating to the financial affairs of the individual	☐ Income ☐ Salary ☐ Benefits ☐ Not applicable ☐ Other – please specify below: Click here to enter text.	Click here to enter text.
Religious or other beliefs of a similar nature	Information relating to the individuals religion or other beliefs	☐ Yes ☐ No ☐ Not applicable List any data items below or attach as an appendix: Click here to enter text.	Click here to enter text.

What data items are being processed e.g. for collection, storage, use and deletion: If there is a chart or diagram to explain please attach as an appendix			
Data Item	**Description**	**Specific data item(s)**	**Justification** Reason that the data items(s) are needed – this must stand up to scrutiny for Caldicott justification
Trade union membership	Information relating to the individuals membership of a trade union	☐ Yes ☐ No ☐ Not applicable List any data items below or attach as an appendix: Click here to enter text.	Click here to enter text.
You must confirm that the data items you have ticked above are relevant and necessary to your project and there is a justified reason for it –if they are not you must amend the above selections to remove those items not relevant/necessary			
Confirm ☐			

Screen 5: Legal Basis for Processing the Data

Is the initiative delivering for Direct Care?

The definition of direct care is: A clinical, social or public health activity concerned with the prevention, investigation and treatment of illness and the alleviation of suffering of individuals. It includes:-

- *supporting individuals' ability to function and improve their participation in life and society*
- *the assurance of safe and high quality care and treatment through local audit,*
- *the management of untoward or adverse incidents*
- *person satisfaction including measurement of outcomes*

undertaken by one or more registered and regulated health or social care professionals and their team with whom the individual has a legitimate relationship for their care

☐ **Yes (go to Q2)** ☐ **No (go to Q1)**

1a. If not Direct care, what is it delivering and how is the consent being obtained	Indirect care • Commissioning ☐ • Monitoring Health and social care ☐ • Public health ☐ • Research ☐ • Other ☐ specify ……
1b. What is the legal basis that permits you to carry this out for indirect care?	Legal basis: • Explicit consent ☐ • Section 251 ☐ • Other legal gateway (please state) ☐ Click here to enter text.

<table>
<tr><td>Informing individuals:
Please state how patients and / or staff will be informed / have been informed of the data collection and processing?</td><td></td></tr>
<tr><td>Information Sharing within UK:
Will personal confidential data be shared with any other organisation?

If yes, please state who the information will be shared with and how and enter in the table:

Is the information from receiving organisation sent back to originating organisation? If yes, please state how the information is transferred back and enter in the table:</td><td>☐ Yes
☐ No

<table><tr><th>From Originator Organisation:</th><th>Data sent to via:</th><th>To Receiving Organisation:</th></tr><tr><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td></tr></table>
<table><tr><th>From Receiving Organisation:</th><th>Data sent back via:</th><th>To Originating Organisation:</th></tr><tr><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td></tr></table></td></tr>
<tr><td>Information Sharing outside the UK:
Will Personal Confidential Data be sent outside the UK?

If yes, please state who the data will be sent to and how?</td><td>☐ Yes
☐ No
..</td></tr>
</table>

Will Personal Confidential Data be sent outside the European Economic Area (EEA)? If yes, please state who the data will be sent to and how?	☐ Yes ☐ No ☐ Not Applicable
Have data protection checks been undertaken to ensure that the non EEA country has adequate data protection / information security standards in place? If yes, please state what checks have been made:	☐ Yes ☐ No ☐ Not applicable
Sending data to the USA?	☐ Yes ☐ No ☐ Not Applicable

Screen 6: Asset / System Information

ICO Notification: If a system is being used, is the Supplier (of this system) registered with the Information Commissioners Office (ICO). If yes, please state their registration number:	☐ Yes ☐ No ☐ Not Applicable (Please specify reason:_____)
DSP Toolkit: Has the Supplier / Third party completed a Data Security & Protection Toolkit Assessment (formerly IG Toolkit) and / or had a ISO27001 accreditation? As regards the DSP Toolkit, please state which version was submitted and if this achieved a satisfactory or non-satisfactory status?	DSP Toolkit completed: ☐ Yes ☐ No DSP Toolkit audited ☐ Yes ☐ No ISO 27001 Accreditation ☐ Yes ☐ No
Contract: Has the third party signed the relevant contract (containing the Information Governance clauses), e.g. NHS E contract / SLA with IG Clause If yes, please state which contract type they have signed up to:	☐ Yes ☐ No

Asset / System Operation:	
Does the asset use privacy invasive technologies for staff and / or patients, e.g. Smartcards? If yes, please state the technology being used:	☐ Yes ☐ No
Will the asset / system process different personal confidential data items which have not been processed previously? If yes, please state the new personal confidential data items to be processed:	☐ Yes ☐ No
Will the asset / system involve new or changed identity authentication requirements that may be intrusive for staff and / or patients? If yes, please state the new identity authentication requirements:	☐ Yes ☐ No
Marketing: Will the asset / system send marketing messages by electronic means? If yes, please state what you are intending to send for marketing purposes:	☐ Yes ☐ No

Have individuals been informed of the marketing and the option to opt in to this?	☐ Yes ☐ No
Automated Decision Making: Is automated decision making to be used within the asset / system? If yes, please briefly describe the process and the reason for it?	☐ Yes ☐ No

Screen 7: System Security and Functions – only to be completed for systems / software

Pseudonymisation / Anonymisation: Can personal confidential data be anonymised or pseudonymised using the system / asset?	☐ Yes ☐ No
Data Quality: How will the personal confidential data be kept up to date and checked for accuracy?	
Access: Who will have access to the system and the personal confidential data? How will access be controlled?	
Auditing: Is there an audit trail for the system? Please can you describe briefly how the audit trail works?	☐ Yes ☐ No

Storage of data: Where will the system information be stored securely?	☐ Within a paper based system stored securely ☐ Within a system / application stored on secure network ☐ Within a database / spreadsheet stored securely on network ☐ Other If Other, please state:
Back Up: <u>Applicable for IT systems only:</u> Are there secure and reliable back up processes in place for the data stored on the system? If yes, please briefly describe what these are. *Please note you may need to contact IT Services for guidance regarding this question*	☐ Yes ☐ No
Retention: Please state the retention periods for the information processed in the system? *Please refer to the Records Management: NHS Code of Practice for Health & Social Care 2016 for assistance with this*.	

Disposal: How will the personal confidential data be disposed of when this is no longer required.	
Training: Each party to confirm that information governance training is in place and all staff with access to personal data have had up to date training	☐ Yes ☐ No

Screen 8: Business Continuity

Do you have a Business Continuity Plan in place if the system and / or process fail or is unavailable for any reason? If yes, briefly describe what the business continuity plan will be in the box:	☐ Yes ☐ No

Screen 9: Additional Comments

Do you wish to supply additional comments about the system / asset? If yes please input comments in box:	☐ Yes ☐ No

Screen 10: Approval and Sign off

PIA Completed by:

Organisation	Name	Date	Signature

Approved by:

Organisation	Name	Date	Signature

Glossary of Terms

Item	Definition
Personal Data	This means data which relates to a living individual which can be identified: A) from those data, or B) from those data and any other information which is in the possession of, or is likely to come into the possession of, the data controller. It also includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual
Sensitive Data	This means personal data consisting of information as to the: A) racial or ethnic group of the individual B) the political opinions of the individual C) the religious beliefs or other beliefs of a similar nature of the individual D) whether the individual is a member of a trade union E) physical or mental health of the individual F) sexual life of the individual G) the commission or alleged commission by the individual of any offence H) any proceedings for any offence committed or alleged to have been committed by the individual, the disposal of such proceedings or the sentence of any court in such proceedings
Direct Marketing	This is “junk mail” which is directed to particular individuals. The mail which are addressed to “the occupier” is not directed to an individual and is therefore not direct marketing. Direct marketing also includes all other means by which an individual may be contacted directly such as emails and text messages which you have asked to be sent to you. Direct marketing does not just refer to selling products or services to individuals, it also includes promoting particular views or campaigns such as those of a political party or charity.