

Data Protection and Confidentiality Policy



Contents

Statement of Intent

Our Vision

1. Introduction
2. Responsible Persons
3. Access to Information
4. Safe and Secure Storage of Files and Data
5. Documentation and Record Keeping
6. Data Protection on the Move
7. Staff Recruitment
8. Checks
9. Shortlisting
10. Interviews
11. Retention of Information
12. Successful Candidates
13. References
14. Gaining Consent
15. Employment Records
16. Pension and Insurance Schemes
17. Equal Opportunities Monitoring
18. Marketing Material
19. Fraud Detection
20. Disclosure Requests
21. Performance Management Records
22. Monitoring the Use of Electronic Communications
23. Information about Employees' Health
24. Sickness and Ill-health Records
25. Occupational Health Schemes
26. Medical Examinations
27. Current Employees
28. Data Protection Impact Assessments (DPIAs) and Biometric Data
29. Artificial Intelligence
30. Personal Data Breach Notification
31. Monitoring and Review
32. Complaints
33. Equality Impact Assessment

Statement of Intent

Our mission is to promote a love of learning in order to maximise the life chances of every child in our Trust. Through our commitment to inclusion, high expectations and skilled teaching, we will have a lasting and positive impact on our local and wider community.

Our Vision

The TEACH Trust supports and nurtures our children to become empowered citizens that make a meaningful contribution to society. Our curriculum reflects our locality and all it offers and aims to educate all children in matters which affect humanity in the wider world: these include all matters that relate to the climate and the world around us, such as climate change; the importance of respecting and celebrating the importance of equality and diversity; and being responsible global citizens.

We have the highest aspirations for our children: the broad and balanced curriculum promotes learning, provides cultural capital and supports spiritual, moral, social and cultural development. The Rights Respecting Gold awards reflects the many ways in which education for character is integral to the work of our schools and highlights our focus on the children's personal development.

We aim to inspire our children to be socially conscious individuals who make a difference to the world. All our children secure the key learning and skills they will need to become lifelong learners and gain employment. Our ultimate aim is to improve all our children's life chances and prepare them to thrive in their future lives.

Under the Equality Act 2010 and the Public Sector Equality Act which came into force in April 2011, the Trust has due regard to the need to eliminate discrimination, advance equality of opportunity and foster good relations.

1. Introduction

The TEACH Trust aims to protect all employees' and pupils right to privacy in line with the *General Data Protection Regulation, the Data Protection Act 2018*, THE Human Rights Act 1998 and the [European Convention of Human Rights](#).

On 28th June 2021, the European Union (EU) formally recognised the UK's high data protection standards as 'adequate'. The trust acknowledges that this allows the continued seamless flow of personal data from the EU to the UK and vice versa. This means that any data product or software in use which stores personal data in the EU or EEA can continue to be used as before, unless the data falls within the scope of the DPA 2018 immigration exemption. The Trust will monitor any updates or changes

to UK-EU adequacy agreements to ensure continued compliance for international transfers.

Personal data of employees, SCITT trainees and candidates will be processed lawfully, fairly and in a transparent manner, collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. The data retained will be accurate and, where necessary, kept up to date, in a form which permits identification of data subjects for no longer than is necessary and processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. The Trust embeds data protection by design and by default into all processing activities and systems.

(Where relevant, the TEACH Trust takes into account any guidance issued by the Local Authority).

The TEACH Trust will register annually with the Information Commissioner's Office.

2. Responsible Persons

The Data Manager of the TEACH Trust (under the guidance of the Data Protection Officer) is responsible for:

- The adherence to data protection law and the safety of processing activities on site;
- Ensuring safe and confidential systems are in place in the TEACH Trust and consulting the Data Protection Officer - Handsam in the implementation, development and monitoring of data processing activities;
- Implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk presented to the personal data processed; and
- Providing information to bodies entitled to receive information under data protection law.

Data Protection Officer- Handsam

- Will ensure that high standards of data security and confidentiality are maintained at all times on site;
- Will coordinate, monitor and oversee appropriate training in data management and encourage a positive data culture;
- Will consult with employees and their representatives with regard to putting data protection procedures in place and monitoring them;
- Will ensure all staff and trainees are aware of the TEACH Trust's data on the move procedures; and

- Will advise on data issues and will assess the severity of data breaches and respond accordingly.
- Can be contacted via email at: info@handsam.co.uk (opening hours 0830-1630 weekdays)

3. Access to Information liaison

All employees, trainees, pupils, and parents/carers have a right to know the nature and source of information kept about them. Each member of staff at the TEACH Trust will be provided with personal details to check regularly, at times determined by the Data Protection Officer.

Employees, trainees, pupils, and parents may make a subject access request at any other time to see the information kept about them in order to verify their accuracy. Employees, trainees, pupils, and parents can make representations to the Data Manager about information being retained that is inaccurate or is of a sensitive personal nature (the right to object, rectification or erasure).

Employees, trainees, pupils, and parents have the right to apply for access to information required for a discipline, capability or grievance hearing (unless the provision of such information might prejudice criminal investigation) in line with the relevant school policies. The records kept should only be sufficient to support conclusions drawn. Unsubstantiated allegations should be removed.

Spent discipline warnings will be removed as detailed in the Disciplinary Policy.

The TEACH Trust will respond to any subject access request without undue delay and provide information within one month. Following receipt of a valid Subject Access Request and satisfactory proof of identity, the Trust will provide the requested information free of charge and within one month. Where requests are complex or numerous, the Trust may extend the compliance period by up to an additional two months. The data subject will be informed of any extension and the reasons for it within one month of receipt of the request.

Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the TEACH Trust reserves the right to either: (a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or (b) refuse to act on the request. The TEACH Trust shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request. Where the TEACH Trust has reasonable doubts concerning the identity of the natural person making the request, the controller may request the provision of additional information necessary to confirm the identity of the data subject.

For further information regarding Subject Access Requests, please refer to DA18 A Guide To The General Data Protection Regulation (GDPR) and UK GDPR / DPA 2018 legislation and Trust SAR .

4. Safe and Secure Storage of Files and Data

The Data Protection Officer will take necessary precautions to ensure that both electronic and manual files are secure.

No manual or electronic files will be taken off the premises except in an emergency, or when expressly authorised by the Data Manager, who will ensure that employees and trainees who are affected are notified and given an opportunity to make representations to him/her. This includes information held on personal computers and portable computing devices, including mobile phones and memory sticks. This list is not exclusive. Employees should refer to the TEACH Trust **Acceptable User policy** that states USB removable storage (that includes SD cards, USB keys and removable hard drives) can all be accessed and read from the Trust computers. The Trust's computer settings will however, ask the user to encrypt any unencrypted storage devices when they are first plugged in. If they refuse, the removable media will show as a read only device and will not allow any documents to be copied or saved onto it.

Manual files will be stored in a safe and secure lockable cabinet at all times. The TEACH Trust will adopt the National Cyber Security Centre's guidance [10 Steps to Cyber Security](#) in the safe and secure storage of electronic files and data. The TEACH Trust will therefore:

- Protect networks from attack and monitor and test security controls in place to achieve this;
- Ensure users are educated, trained and aware;
- Produce and establish anti-malware defences across the school;
- Apply security patches and ensure secure configuration of all systems is maintained;
- Establish effective management processes, limit user privileges and monitor user activity appropriately;
- Establish an incident response and disaster recovery capability;
- Establish an effective monitoring strategy of all systems and networks; and
- Develop and implement a policy on the use of mobile phones and train staff to adhere to it.

5. Documentation and Record Keeping

Under the *General Data Protection Regulation*, records of processing must be retained. The TEACH Trust will hold compliant and comprehensive processing records in relevant fields, covering the nature of the data, the purposes of processing, any recipients, security measures, retention times and controller information.

6. Data Protection on the Move

The loss of data outside the immediate school environment can be the most serious and costly.

The Data Protection Officer for the TEACH Trust will ensure that all staff are aware of the dangers of taking data off the school's immediate environment and are aware of the procedures in place to minimise the risk.

All devices storing data such as laptops and any work phones must be password protected and data encrypted. Staff will not remove any more data than is necessary from the TEACH Trust premises. TEACH Trust employees must refer to the Bring Your Own Device Policy which states all mobile devices used off site must be encrypted and secured. Window devices are secured with Bitlocker and all other mobile devices will be secured with a 6-character password where possible.

Any email containing sensitive personal data (special category data) (either in the body or within an attachment) should be sent as an encrypted email by including Encrypt in the subject line. Any emails sent from a @teachpoole.com to a @teachpoole.com address is automatically encrypted.

7. Staff Recruitment

In advertising for posts, the TEACH Trust will include a privacy notice detailing what personal data or sensitive personal data will be gathered, how it will be held, processed and disposed of. The notice will also inform individuals of their data rights. See example extract below:

“Personal information provided by candidates will be securely filed electronically and password protected and paper copies locked in filing cabinets in a locked office. They will not be released to third parties outside the school without the consent of the person concerned, except where there is a legal requirement to do so. If the application does not proceed, the data will be securely disposed of after 6 months. Any concerns regarding data gathered in the recruitment process should be directed to the Data Manager – Hayley Hemmings at h.hemmings@teachpoole.com

Within the TEACH Trust the Data Manager will determine who may have limited access to this information and will inform the person(s) concerned that this is being done.

The TEACH Trust will not collect more personal information than is necessary for the recruitment process. Information collected will not be irrelevant or excessive.

8. Checks

Disclosure and Barring Service (DBS) checks will be carried out in line with statutory responsibilities under the *Safeguarding Vulnerable Groups Act 2006*, as amended by

the *Protection of Freedoms Act 2012* and statutory guidance in [Keeping Children Safe in Education](#).

Any other vetting which is required by law will be carried out as necessary and in line with current legislation and policy.

Checks to verify the qualifications and fitness to teach (or to support teaching) will also be carried out. Other checks may be carried out to verify information provided by candidates for posts or for places on the SCITT PGCE course.

9. Shortlisting

Candidates will be informed that the selection panel will have access to the information provided in the application and any references received.

In line with KCSIE, online searches *will be undertaken on all shortlisted candidates*.

10. Interviews

Only the information relevant to the recruitment process (and information that may be required in defence against any discrimination claims) will be retained after the interview (application forms, interview question notes and references). Candidates will be told which information will be retained.

All other interview material will be destroyed immediately after the interview.

11. Retention of Information

Data is held in accordance with the IRMS Retention policy. Data is held securely in paper copy, on electronic systems, and in a cloud based secure area. See the Trust's Privacy Notices for further information.

TEACH will only retain the data we collect for as long as is necessary to satisfy the purpose for which it has been collected.

The information of unsuccessful candidates obtained for recruitment purposes at the TEACH Trust will be retained for 6 months before secure disposal. For SCITT trainee applicants who are unsuccessful, information will be retained until the end of the current recruitment cycle.

A secure central record that will list all checks carried out will be kept for the purposes of inspection and to assure Trustees that records have been checked.

12. Successful Candidates

On assumption of a role at the TEACH Trust the forms of personal data which will need to be processed and gathered for the performance of the role will be outlined to the individual in a privacy notice as part of their induction. This data will include verified

references obtained during the recruitment process and an up to date DBS check. This data will be securely held for 6 years after termination of employment. For successful SCITT trainees, data will be held securely for 7 years after they finish the PGCE course.

13. References

Candidates do not have the right to obtain access to a confidential reference from the school/organisation giving it, but no such exemption exists for the prospective employer unless the reference was provided in confidence and falls under the Schedule 2 exemption of the DPA 2018.

The TEACH Trust will not provide confidential references to other institutions/organisations about an employee at the TEACH Trust unless the employee requests one in writing for good reason.

14. Gaining Consent

Where required, requests for consent to personal data processing will be intelligible, easily accessible, in plain language and with the purpose for the data processing stated and evident. Consent will cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent will be gathered for all of them.

The TEACH Trust acknowledges that special categories of personal data require explicit consent and that contractual necessity or compliance with law also serve as mechanisms for processing personal data.

Consent gathered will be held securely in a clear and auditable form. Subjects will be able to be withdraw consent through the same media it was given. If consent is withdrawn, this does not necessarily make the processing unlawful, this must be noted if applicable in the consent request.

15. Employment Records

The TEACH Trust aims to balance its need to keep records and the employee's and trainee's right to a private life.

16. Pension and Insurance Schemes

Information may be supplied to a third party for pensions and insurance schemes, where such information is necessary. Pension enrolment is automatic so opting out authorisation must be secured from employees who do not wish to enrol.

17. Equal Opportunities Monitoring

Information on staff is periodically required by the government (or, where relevant, LA). This is sensitive personal data, and the information will be kept to a minimum, and as far as possible, in an anonymous form. The Data Protection Officer will ensure that high standards of data security and confidentiality are maintained at all times. Staff will

have a full awareness of this form of personal data processing on assumption of job role through contract and privacy notice.

18. Marketing Material

No information about employees or trainees at the TEACH Trust will be provided to marketing companies, unless the person(s) concerned have given explicit and auditable consent.

19. Fraud Detection

Data matching for fraud detection (e.g. to detect whether the employee is receiving state benefits or not) are possible. Before the employer consents to the school participating in such a scheme, the staff will be consulted. New employees must then be told of this scheme, and all employees should be reminded of it periodically under arrangements made by the Data Protection Officer and approved by the employer.

20. Disclosure Requests

Members of staff who receive requests for references or other information about members of the current or previous employees at the TEACH Trust should ensure they are saved on the HR system and that the Data Manager is informed before providing the information to ensure that they are acting within the law and official guidance.

21. Performance Management Records

Performance reviews will be carried out on all staff in accordance with the TEACH Trust Performance Management Policy.

The reports on teaching staff performance obtained through the annual formal performance management system will be retained by the HR department (with a copy to the member of staff concerned). Only details about professional development needs/requests may be shared with other staff.

The TEACH Trust has the same arrangements in place for performance records of all staff.

22. Monitoring the Use of Electronic Communications

The Trust Board will keep all monitoring at work within the provisions of the General Data Protection Regulation and the European Convention of Human Rights.

The TEACH Trust will not intrude into the private lives of staff, trainees or pupils, however, it does reserve the right to ensure they uphold their duties as outline in Part Two of the National Teachers' Standards (2011) DFE-00066-2011. In addition, pupils are expected to behave on social media in a way that does not breach the law or bring the school/Trust into disrepute. The Trust reserves the right to monitor the use of all electronic devices issued or made available by the TEACH Trust, such as school computers, laptops, video and audio machines, phones and fax machines. This will

only be done where there is a good reason to do so and appropriate records will be kept, which can be accessed by staff (and pupils) on request to the Data Manager.

All monitoring will be conducted in accordance with the powers of an employer under the *Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000*, and in accordance with the Department for Education's statutory guidance *Keeping Children Safe in Education (KCSIE)*, including the requirements relating to filtering and monitoring standards.

which permits an employer to vet communications without the consent of the caller, writer or recipient where the intention is:

- To establish the existence of facts applicable to the business;
- To ascertain compliance with regulatory or self-regulatory practices or procedures which are applicable to the system controller in the carrying on of his business, or applicable to another person in the carrying on of his business where that person is supervised by the system controller in respect of those practices or procedures;
- To ascertain or demonstrate the standards which are achieved or ought to be achieved by persons using the system in the course of their duties;
- In the interest of national security;
- For the purpose of preventing or detecting crime;
- For the purpose of investigating or detecting the unauthorised use of that or any other telecommunication system;
- In order to secure or as an inherent part of the effective operation of the system;
- Monitoring communications for the purpose of determining whether they are communications relevant to the system controller's business; and
- Monitoring communications made to a confidential voice-telephony counselling or support service which is free of charge (other than the cost, if any, of making a telephone call) and operated in such a way that users may remain anonymous if they so choose.

All staff and trainees are advised that such monitoring might take place at the TEACH Trust for these purposes including for the misuse of school equipment or its use for inappropriate purposes.

The employer will establish with the Data Protection Officer after consultation with the staff, a policy on how telephones/fax and computers may be used for any private communications. Breach of this code once established will be a discipline offence.

23. Information about Employees' Health

The TEACH Trust understands that under the *General Data Protection Regulation*, data relating to an individual's health is sensitive. Data relating will be managed with a constant awareness of data protection in a confidential and secure manner. Concerns regarding how data is managed should be reported to the Data Manager.

Any data on an employee's or trainee's state of physical or mental health is sensitive personal data and will only be kept when the employee or trainee has been told what information is involved and the use that will be made of it, and the arrangements for its security. At the employee's or trainee's request, and if required, the Trust may hold sensitive information about an employee's or trainee's health as part of a confidential care plan. The information will not be retained without the employee's or trainee's written auditable consent to its retention. Only necessary and limited individuals at the TEACH Trust will be able to access this information where they genuinely need it to carry out their job.

24.Sickness and Ill-health Records

As far as possible, the TEACH Trust will only retain information that is necessary to establish an employee's fitness for work or fitness to '*train to teach*' in the case of SCITT trainees. The employer has delegated to Data Protection Officer the responsibility for determining what is necessary.

The TEACH Trust recognises the difference between a 'sickness or injury record' and an 'absence record'.

Sickness or injury records contain sensitive personal information. They will only be kept for specific purposes with the written auditable consent of the employee or trainee, e.g. in the case of capability or absence through ill-health proceedings. However, this does not prevent the TEACH Trust from recording that sickness notes have been received and the dates of the absence. The following retention periods apply;

Sickness absence monitoring records - 5 years after period of sickness,

Record of Return to Work Interviews - 5 years after period of sickness,

Sickness Records for Payroll Purposes – 6 financial years + current financial year

Staff absences are recorded on the Trust HR system detailing the absence category. The employee provides further information regarding their absence during their Return to Work interview with their Line Manager. This is also recorded on the Trust HR system by the Headteacher or CEO. SCITT trainee absences are recorded at the SCITT office.

No information about any of the above records will be made available to any other employees unless cleared by the Data Manager as necessary.

Requests for information from doctors and other medical practitioners will be in accordance with the *Access to Medical Reports Act 1998*.

25.Occupational Health Schemes

The TEACH Trust will operate within the rules of any scheme to which it belongs. All staff will be informed about how health information will be used under the scheme and

who will have access to it. A processing agreement with the scheme will be secured to this end.

Details are contained in the Standard Statement of Appointment Conditions.

26. Medical Examinations

Recruitment

Job applicants must only be medically examined to:

- Ensure they are medically fit for the specific role;
- Meet legal requirements; and
- Determine the terms on which they are eligible to join a pension or insurance scheme.

The TEACH Trust will make it clear during the recruitment process if tests are required for the role.

27. Current Employees & trainees

Medical information will only be obtained through examination or testing if:

- The tests are part of a voluntary occupational health and safety programme;
- Necessary to prevent a significant health risk;
- Needed to determine an employee's or trainee's continuing fitness for the role;
- Needed to determine whether an employee or trainee is fit to return to work (or train) after a period of absence;
- Needed to determine an employee's entitlement to health-related benefits; or
- Needed to prevent discrimination on the grounds of disability, or to assess the need to make reasonable adjustments, or to comply with other legal obligations.

28. Data Protection Impact Assessments (DPIAs) and Biometric Data

The Trust will carry out a Data Protection Impact Assessment (DPIA) whenever it intends to process personal data in a way that is likely to result in a high risk to the rights and freedoms of individuals. This may include the introduction of major new IT systems, CCTV surveillance, or large-scale processing of special category data.

Where biometric data is used (for example, fingerprint scanning for catering or access control), the Trust will comply fully with sections 26 to 28 of the Protection of Freedoms Act 2012. Written consent will be obtained from at least one parent/carer before the biometric data of a child is collected and processed. If a pupil objects to, or refuses, the use of biometric data, an alternative non-biometric method will be provided immediately.

29. Artificial Intelligence (AI)

The Trust recognises that Artificial Intelligence (AI), including generative AI tools, can support teaching, learning and administrative functions when used appropriately.

Any use of AI within the Trust must comply with the UK GDPR, Data Protection Act 2018, safeguarding requirements and all relevant Trust policies.

Staff, Trustees and other authorised users must only use AI tools that have been approved by the Trust and must adhere to the requirements set out in the Trust's AI Policy. Personal, confidential, special category or otherwise identifiable information must not be entered into open AI platforms or tools unless expressly authorised by the Trust and protected through appropriate contractual, technical and organisational safeguards.

All AI-generated content remains the responsibility of the individual using the tool. Information produced by AI must be reviewed for accuracy, appropriateness, bias, safeguarding concerns and compliance with legal and professional obligations before being relied upon or shared.

Any suspected data breach, unauthorised disclosure of personal data, or safeguarding concern arising from the use of AI must be reported immediately to the Data Manager, Data Protection Officer and, where appropriate, the Designated Safeguarding Lead, in accordance with Trust procedures.

The Trust will regularly review its use of AI technologies and will undertake Data Protection Impact Assessments (DPIAs) where required to ensure emerging technologies continue to be used safely, ethically and lawfully.

30. Personal Data Breach Notification

A personal data breach is a breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

All staff must report any suspected personal data breach to the Data Manager and Data Protection Officer (DPO) immediately upon becoming aware of it.

Where a personal data breach is likely to result in a risk to the rights and freedoms of individuals, the Trust will notify the Information Commissioner's Office (ICO) without undue delay and, where required, within 72 hours of becoming aware of the breach.

Where the breach is likely to result in a high risk to individuals, the Trust will also inform the affected data subjects without undue delay.

31. Monitoring and Review

The CEO and the Trust Board will monitor the implementation of the policy and check annually that the TEACH Trust has registered with the Information Commissioner's Office.

The CEO and the Data Manager will monitor the effectiveness of the policy and will report to Trustees at least annually.

The Compliance and Pupil Safeguarding Committee will review this policy at least every two years and assess its implementation and effectiveness. The policy will be promoted and implemented throughout the school.

Alongside the TEACH Trust Data Protection Policy, please also refer to;

- TEACH Trust Bring Your Own Device Policy
- TEACH Trust Code of Practice for Use of Computers Policy
- TEACH Trust Acceptable User Policy
- TEACH Trust Remote Access Policy
- TEACH Trust Staff Laptop Agreement

Date reviewed September 2026

Next review date: September 2027

Data Protection Officer: Handsam (info@handsam.co.uk)

Data Manager: Hayley Hemmings (h.hemmings@teachpoole.com)

32. Complaints

We take any complaints about how we collect and use personal information very seriously. If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concerns about our data processing, please raise this with us in the first instance. You can make a complaint to us at any time by contacting Mrs Hayley Hemmings, the Trust Data Manager on h.hemmings@teachpoole.com

Upon receiving a complaint, we will:

- Acknowledge receipt of the complaint within WITHIN 5 WORKING DAYS days of receiving it
- Without undue delay, take appropriate steps to respond to the complaint, including:
- Make appropriate enquiries based on the circumstances of the complaint
- Keep the complainant informed on the progress of the investigation
- Without undue delay, inform the complainant of the outcome of the investigation within one calendar month of receipt.

33 Equality Impact Assessment

Question	Response	
		Please tick
Which relevant groups and stakeholders have been consulted with in relation to this policy?	Pupils	✓
	Trustees	✓
	Staff	✓
	Poole SCITT (employees and students)	✓

	Parents/Carers	
	Local Authority	✓
	Trade Unions	
	Other Advisors (give details)	Handsam. Health & Safety Coordinator
What are the arrangements for monitoring and reviewing the actual impact of the policy?	Termly	
	Annually	
	When applied	Every 2 years
	If legislation changes	✓
	If a formal complaint	

Does the policy affect one group less or more favourably than another on the basis of:	Y/N
Disability	N
Gender reassignment	N
Marriage or civil partnership	N
Pregnancy and maternity	N
Race	N
Religion or belief	N
Sexual orientation	N
Sex (gender)	N
Age	N
SEN	N
Vulnerable	N
Traveller, migrant, refugees and people seeking asylum	N
EAL	N

	Y/N	Comments/Actions
Is there any evidence that some groups are affected differently?	N	
If you have identified potential discrimination, are any exceptions valid, legal and/or justifiable?	N/A	
Is the impact of the policy likely to be negative?	N	
If yes, can the impact be mitigated by taking different action?	N/A	