Heartlands Community Trust

Data Protection Policy

Circulated for consultation:	**N/A**	
Approved By	**Directors Meeting**	**15 July 2018**
Signed	**Simon Garrill** **Chief Executive Officer**	**Jeff Twentyman** **Chair of Directors**

Contents

1. Aims

1.1 Heartlands Community Trust (the "Trust") is a multi-academy trust (MAT), and aims to ensure that all personal data collected about staff, students, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.

1.2 This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Legislation and guidance

2.1 This policy meets the requirements of the GDPR and the *expected* provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.

2.2 It meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data.

2.3 It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

2.4 In addition, this policy complies with the Trust's master funding agreement and articles of association.

3. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's:

	• Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. The data controller

4.1 The Trust processes personal data relating to parents, students, staff, governors, visitors and others, and therefore is a data controller.

4.2 The Trust is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

5. Roles and responsibilities

5.1 This policy applies to **all staff** employed by the Trust, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy *may* face disciplinary action.

The Board of Directors (the Board)

5.2 The Board has overall responsibility for ensuring that the Trust complies with all relevant data protection obligations.

Data protection officer

5.3 The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

5.4 They will provide an annual report of their activities directly to the Board and, where relevant, report to the Board their advice and recommendations on Trust/school data protection issues.

5.5 The DPO is also the first point of contact for individuals whose data the Trust processes, and for the ICO.

5.6 Full details of the DPO's responsibilities are set out in their job description.

5.7 Our DPO is Leslie Boodram (Chief Finance Officer) and is contactable via 0208 826 1230 x 395.

Head of School

5.8 The Head of School acts as the representative of the data controller on a day-to-day basis.

All staff

5.9 Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing their school of any changes to their personal data, such as a change of address
- Contacting the DPO in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - If they have any concerns that this policy is not being followed
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area

- If there has been a data breach
- Whenever they are engaging in a new activity that may affect the privacy rights of individuals
- If they need help with any contracts or sharing personal data with third parties

6. Data protection principles

6.1 The GDPR is based on six (6) data protection principles that The Trust must comply with. The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

6.2 This policy sets out how the school aims to comply with these principles.

7. Collecting personal data

Lawfulness, fairness and transparency

7.1 The Trust will only process personal data where it has one of six 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the Trust can **fulfil a contract** with the individual, or the individual has asked the Trust to take specific steps before entering into a contract
- The data needs to be processed so that the Trust can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life
- The data needs to be processed so that the Trust, as a public authority, can perform a task **in the public interest** (or public task), and carry out its official functions
- The data needs to be processed for the **legitimate interests** of the Trust or a third party (provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/carer when appropriate in the case of a student) has freely given clear **consent**

7.2 The majority of Trust business will be undertaken under public interest or consent.

7.3 For special categories of personal data (see section 3), the Trust will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018. Accordingly:

- With regard to primary schools, if the Trust offers online services to students, such as classroom apps, and intends to rely on consent as a basis for processing, the Trust will get parental consent (except for online counselling and preventive services).
- With regard to secondary schools, if the Trust offers online services to students, such as classroom apps, and intends to rely on consent as a basis for processing, it will get parental consent where the student is under 16 years old (except for online counselling and preventive services).

7.4 Whenever the Trust first collects personal data directly from individuals, it will provide them with the relevant information required by data protection law.

Limitation, minimisation and accuracy

7.5 The Trust will only collect personal data for specified, explicit and legitimate reasons. It will explain these reasons to the individuals when it first collects their data.

7.6 If the Trust wants to use personal data for reasons other than those given when it first obtained it, the Trust will inform the individuals concerned before it does so, and seek consent where necessary.

7.7 Staff must only process personal data where it is necessary in order to do their jobs.

7.8 When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. (stored and/or archived). This will be done in accordance with the Trust records retention policy.

8. Sharing personal data

8.1 The Trust will not normally share personal data with anyone else, but may do so where:

- There is an issue with a student or parent/carer that puts the safety of its staff at risk
- It needs to liaise with other agencies – the Trust will seek consent as necessary before doing this
- Its suppliers or contractors need data to enable it to provide services to its staff and students – for example, IT companies. When doing this, the Trust will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law

- Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data the Trust may share
- Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

8.2 The Trust will also share personal data with law enforcement and government bodies where it is legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

8.3 The Trust may also share personal data with emergency services and local authorities to help them to respond to an emergency that affects any of its students or staff.

8.4 Where the Trust transfer personal data to a country or territory outside the European Economic Area, it will do so in accordance with data protection law.

9. Subject access requests and other rights of individuals

Subject access requests

9.1 Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

9.2 Subject access requests must be submitted in writing, either by letter, email or fax to the DPO. They should include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

9.3 If staff receive a subject access request they must immediately forward it to the DPO.

9.4 A subject access request form is at Annex A, and shown separately on the Trust websites.

Children and subject access requests

9.5 Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent. Therefore:

- Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of students at our school may be granted without the express permission of the student. This is not a rule and a student's ability to understand their rights will always be judged on a case-by-case basis.
- Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of students at our school *may* not be granted without the express permission of the student. This is not a rule and a student's ability to understand their rights will always be judged on a case-by-case basis.

Responding to subject access requests

9.6 When responding to requests, the Trust:

- May ask the individual to provide two (2) forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within one (1) month of receipt of the request
- Will provide the information free of charge
- May tell the individual it will comply within three (3) months of receipt of the request, where a request is complex or numerous. The Trust will inform the individual of this within (1) one month, and explain why the extension is necessary

9.7 The Trust will not disclose information if it:

- Might cause serious harm to the physical or mental health of the student or another individual

- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

9.8 If the request is unfounded or excessive, the Trust may refuse to act on it, or charge a reasonable fee, which takes into account administrative costs.

9.9 A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information.

9.10 When the Trust refuses a request, it will tell the individual why, and tell them they have the right to complain to the ICO.

Other data protection rights of the individual

9.11 In addition to the right to make a subject access request (see above), and to receive information when the Trust is collecting their data about how it uses and processes it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask the Trust to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

9.12 Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

10. Parental requests to see the educational record

10.1 Those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a student) within 20 school days of receipt of a written request.

11. Biometric recognition systems

11.1 Where The Trust uses students' biometric data as part of an automated biometric recognition system (for example, students use fingerprints to receive school dinners instead of paying with cash), the Trust will comply with the requirements of the Protection of Freedoms Act 2012[1].

11.2 Parents/carers will be notified before any biometric recognition system is put into a new school or before their child first takes part in it. In that instance, the Trust will get written consent from at least one parent or carer before it takes any biometric data from their child and first processes it.

11.3 Parents/carers and students have the right to choose not to use the school's biometric system(s). The Trust will provide alternative means of accessing the relevant services for those students. For example, students can pay for school dinners in cash at each transaction if they wish

11.4 Parents/carers and students can object to participation in the school's biometric recognition system(s), or withdraw consent, at any time, and the Trust will make sure that any relevant data already captured is deleted.

11.5 As required by law, if a student refuses to participate in, or continue to participate in, the processing of their biometric data, the Trust will not process that data irrespective of any consent given by the student's parent(s)/carer(s).

11.6 Where staff members or other adults use the school's biometric system(s), the Trust will also obtain their consent before they first take part in it, and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the school will delete any relevant data already captured.

12. CCTV

12.1 Where the Trust uses CCTV in various locations around the MAT to ensure it remains safe. The Trust will adhere to the ICO's code of practice for the use of CCTV.

---

[1] *In the context of the Protection of Freedoms Act 2012, a "child" means a person under the age of 18.*

12.2 The Trust does not need to ask individuals' permission to use CCTV, but makes it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

12.3 Any enquiries about the CCTV system should be directed to Anthony Latchana, School Business Manager.

13. Photographs and videos

13.1 As part of school activities, the Trust may take photographs and record images of individuals within the schools.

13.2 With regard to Primary schools, the Trust will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials, and will clearly explain how the photograph and/or video will be used to both the parent/carer and student.

13.3 With regard to secondary schools, the Trust will obtain written consent from parents/carers, or students aged 18 and over, for photographs and videos to be taken of students for communication, marketing and promotional materials. Where parental consent is required, the Trust will clearly explain how the photograph and/or video will be used to both the parent/carer and student. Where parental consent is not required, the Trust will clearly explain to the student how the photograph and/or video will be used.

13.4 Uses may include:

- Within school on notice boards and in school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns, prospectus
- Online on our school website or social media pages

13.5 Consent can be refused or withdrawn at any time. If consent is withdrawn, the Trust will delete the photograph or video and not distribute it further.

13.6 When using photographs and videos in this way the Trust will not accompany them with any other personal information about the child, to ensure they cannot be identified.

13.7 Further information can be obtained from the Trust's child protection and safeguarding policy and social media regarding use of photographs and videos.

14. Data protection by design and default

14.1 The Trust will put measures in place to show that it has integrated data protection into all data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing data protection impact assessments (DPIA) where the Trust's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process). In discharging this obligation, the Trust will use both data screening and a risk assessment template – as shown at Annex B
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; the Trust will also keep a record of attendance
- Regularly conducting reviews and audits to test Trust privacy measures and to ensure compliance
- Maintaining records of Trust processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our schools and DPO and all information that is required to share about how the Trust uses and processes their personal data (via privacy notices)
    - For all personal data held, maintaining an internal record of the type of data, data subject, how and why the Trust is using the data, any third-party recipients, how and why the Trust is storing the data, retention periods and how the Trust is keeping the data secure

15. Data security and storage of records

15.1 The Trust will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

15.2 In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use

- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access. For the avoidance of doubt, the Trust will operate controlled access systems
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and students are reminded to change their passwords at regular intervals
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices. Staff, students or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our [online safety policy/ICT policy/acceptable use agreement/policy on acceptable use])
- Where the Trust needs to share personal data with a third party, it carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

16. Disposal of records

16.1 Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where the Trust cannot or do not need to rectify or update it.

16.2 For example, the Trust will shred or incinerate paper-based records, and overwrite or delete electronic files. It may also use a third party to safely dispose of records on the Trust's behalf. And if it does so, it will require the third party to provide sufficient guarantees that it complies with data protection law.

17. Personal data breaches

17.1 The Trust will make all reasonable endeavours to ensure that there are no personal data breaches.

17.2 In the unlikely event of a suspected data breach, the Trust will follow the procedure set out in Annex C.

17.3 When appropriate, the Trust will report the data breach to the ICO within ***72 hours***. Such breaches in a school context may include, but are not limited to:

- A non-anonymised dataset being published on the school website which shows the exam results of students eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person

- The theft of a school laptop containing non-encrypted personal data about students

17.4 The Trust will ensure that any breach is fully investigated by the DPO using the template at Annex D. All breaches will be listed on a data breach log.

18. Training

18.1 All staff and governors are provided with data protection training as part of their induction process.

18.2 Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

19. Monitoring arrangements

19.1 The DPO is responsible for monitoring and reviewing this policy.

19.2 This policy will be reviewed and updated if necessary when the Data Protection Bill receives royal assent and becomes law (as the Data Protection Act 2018) – if any changes are made to the bill that affect Trust practice.

19.3 Due to the inception of the GDPR, this policy will be reviewed in one (1) year (i.e. July 2019) and in two[2] (2) yearly cycles thereafter (July 2021), or until such time as another school joins the MAT or legislation/regulation change, whichever is the sooner.

20. Links with other policies

20.1 This data protection policy is linked to:

- Freedom of information publication scheme
- ICT acceptable use policy
- ICT data storage and retention policy
- Safeguarding policy
- Policy on the use of photographs and videos, etc.

[2] *Note: the 2-year review frequency here reflects the information in the Department for Education's advice on statutory policies.*

Annex A : Subject Access Request Form

The Data Protection Act 2018 provides you, the data subject, with a right to receive a copy of the data/information we hold about you or to authorise someone to act on your behalf. Please complete this form if you wish to see your data. You will also need to provide proof of your identity. Your request will be processed within thirty (*30) calendar days* upon receipt of a fully completed form and proof of identity.

Proof of identity:

We require proof of your identity before we can disclose personal data. Proof of your identity should include a copy of two (2) documents such as your birth certificate, passport, driving licence, official letter addressed to you at your address e.g. bank statement, recent utilities bill or council tax bill. The documents should include your name, date of birth and current address. If you have changed your name, please supply relevant documents evidencing the change. We may contact you to confirm that this request was made

Administration fee:

Heartlands Community Trust's policy is not to charge for Subject Access Requests (except where the conditions in section 9.8 prevail)

Section 1

Please fill in your details (the data subject). If you are not the data subject and you are applying on behalf of someone else, please fill in the details of the data subject below and not your own.

Title: Mr ☐ Mrs ☐ Ms ☐ Miss ☐ Other – (please state)
Surname/Family Name:
First Name(s)/Forename:
Date of Birth:
Address :
Postcode:
Previous Address:
Postcode
Day Time Telephone Number:
Email:

I am enclosing the following two (2) copies as proof of identity:

Birth certificate ☐ Driving Licence ☐ Passport ☐ An official letter to my address ☐

If none of these are available please contact the Data Protection Officer on 020 8826 1230

Personal Information

Please use the space below to provide further details to help locate the information sought. For example, the Trust school, specific documents or information that you are seeking; department if known, the areas of the school records that you wish this subject access request to cover; the name of the person who may have created or had access to the information, if known; and any relevant time periods. Please be as precise as possible and provide dates of interest to be covered by this subject access request.

Details:

Employment records ☐

If you are now, or have been employed by the Trust and are seeking personal information in relation to your employment please provide details of your Staff number/Programme/Pool/Dates of employment.

Section 2

Please complete this section of the form with your details if you are acting on behalf of someone else (i.e. the data subject).

If you are NOT the data subject, but an agent appointed on their behalf, you will need to provide evidence of your identity as well as that of the data subject and proof of your right to act on their behalf.

Title: Mr ☐ Mrs ☐ Ms ☐ Miss ☐ Other – (please state)
Surname/Family Name:
First Name(s)/Forename:
Date of Birth:
Address:
Postcode:
Day Time Telephone Number:
Email:

Please provide proof of identity as detailed on section 1

I am enclosing the following copies as proof of identity: Birth certificate ☐ Driving Licence ☐ Passport ☐ An official letter to my address ☐
If none of these are available please contact the Data Protection Officer on 020 8826 1230
What is your relationship to the data subject? (e.g. parent, carer, legal representative)
I am enclosing the following copy as proof of legal authorisation to act on behalf of the data subject Letter of authority ☐ Lasting or Enduring Power of Attorney ☐ Evidence of parental responsibility ☐ Other(give details)

Data Subject Declaration : **I certify that the information provided on this form is correct to the best of my knowledge and that I am the person to whom it relates. I understand that Heartlands Community Trust is obliged to confirm proof of identity/authority and it may be necessary to obtain further information in order to comply with this subject access request.**
Name:
Signature:
Date:
OR
Authorised person – Declaration (if applicable): **I confirm that I am legally authorised to act on behalf of the data subject. I understand that Heartlands Community Trust is obliged to confirm proof of identity/authority and it may be necessary to obtain further information in order to comply with this subject access request.**
Name:
Signature:
Date:

Your Checklist	
Is your contact information correct?	
Have you enclosed acceptable identification?	
Have you signed the form?	
Have you completed all the sections?	
Have you provided accurate detail to enable us to find the information?	

SAR Checklist- for Heartlands Community Trust			
Date of application received		Information found	
Identification (1) details		Application complete	
Identification (2) details		Information sent by post	
Application signed			

Submission

When you have completed the form, please send it together with your proof of identity to:

Attn: Leslie Boodram
The Data Protection Officer
Heartlands Community Trust
Station Road
London N22 7ST

Forms that are incomplete will be returned for the person to complete in more detail, together with an explanation for the form being returned to you.

Annex B : Data Protection Impact Assessment (Part A: Screening Questions)

The GDPR requires controllers to carry out data protection impact assessments (DPIAs) when:

- using new technologies; and
- processing is likely to result in high risk to the rights and freedoms of individuals.

Processing that is likely to result in high risk includes (but is not limited to):

- Systematic and extensive processing activities, including profiling where decisions have legal effects – or similar significant effects – on individuals.
- Large scale processing of special categories of data (all data known as sensitive personal data under the Data Protection Act 1998 plus genetic and biometric data) or personal data relating to criminal convictions or offences.
- Large scale systematic monitoring of public areas (e.g. CCTV).

Effectively, when looking at processing activities (i.e. processing any personal data held), and whether the new system/software may put the individuals at risk – either because there is a risk that their data may be revealed or disclosed, or there is a risk of an invasion into privacy (such as with CCTV systems), then a DPIA is required.
Where the DPIA indicates that any planned processing would be of high risk in the absence of risk-mitigating measures taken by the controller, the controller is required to consult the supervisory authority (the ICO) prior to proceeding.

In order to ensure that the Trust puts Risk Assessments in place when required, it utilizes a series of **Screening Questions**, which are detailed below. Positive responses indicate the need for a full Risk Assessment (Annex D). ***All DPIAs at the Heartlands Community Trust are approved (or otherwise) by our Data Protection Officer***

Screening question	Response	Response
Will the project involve the collection of new information about individuals?	Yes	No
Will the project compel individuals to provide information about themselves?	Yes	No
Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	Yes	No
Are you using information about the individual for a purpose that it is not currently used for, or in a way that it is not currently used?	Yes	No
Does the project involve using new technology which might be perceived as being privacy-invasive?	Yes	No

Is the information about individuals or a kind particularly likely to raise privacy concerns or expectations?	Yes	No
Will the project require you to contact individuals in ways which they might find intrusive?	Yes	No

Note that answering 'yes' to any of these questions is an indication that a Data Protection Impact Assessment (DPIA) would be a useful exercise.
Not all projects will require the same level of DPIA. Should the outcome of the screening be that a full DPIA is not required, a copy of this form will be retained.
Finally, should special category personal data be collected or used, additional safeguards will need to be in place.

Annex B : Data Protection Impact Assessment (Part B: Risk assessment template)

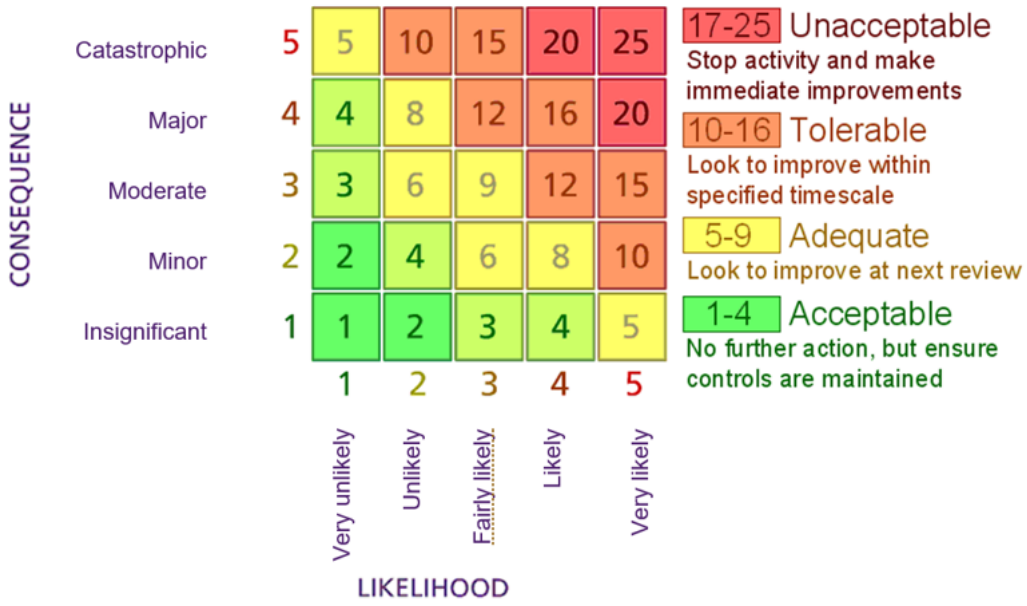
Data Processing activity - question	Score Confidence	Score Likelihood	Overall Score (C x I)	Response	Risk mitigation in place
What is it that you want to do with the data? *(Here, you need to identify what it is you want to do, in as much detail as you can. Describe what information is collected or used, what it is used for, who it is obtained from and disclosed to, who will have access to it and how many people are affected. As an example, if you are installing CCTV, can you say how many cameras and where? Which data subjects will be affected? What use will be made, and by whom? What are the views of the general public on this type of operation?)* *From this you must identify risks*					

What are the benefits of what you are doing? *(Why are you considering the action identified above? What benefits will it bring to you? What are you likely to gain from it? Why do you consider it necessary? There must be a legitimate interest being pursued in a necessary and proportionate way.*					
What are the risks to the rights and freedoms of data subjects? *(What is the likely impact on individuals if you implement the course identified above? What risks exist to the individual? What is the likely impact on the individual's general right to privacy? Have you consulted, internally and externally, to identify and address privacy risks?)*					

What steps can you take to mitigate the risks identified above? *(Having identified the risks, is there anything that you can do to mitigate those risks? List everything that you could do – even if it is something that you will not end up implementing. Identify how the action mitigates the risk, and whether you would consider it a possibility, having regard to the purpose of what you are considering doing. Include any future steps that may be necessary – for example future security testing. Do you need to amend your privacy notices?) Cover safeguards, security measures and mechanisms to ensure the protection of personal data.*					
Should we consult with data subjects before taking this step? *(Who are the relevant data subjects? Can they participate in the consultation effectively? What process will you use to take account of any views expressed?)*					

Do the benefits outweigh the risks, taking into account any mitigation that you will put in place? *(This is the final conclusion – set out whether the benefits outweigh the risks first, and your reasons for reaching this conclusion. Relevant to this will be an analysis of the potential steps you could take to mitigate, and identify which of those you will implement, and why. The mitigated impact on individuals must be necessary and proportionate to the aim you set out to achieve.)*					
How will the DPIA be given effect? *(How are the mitigation steps and other measures under the DPIA to be built into the project and who will be responsible for ensuring they are carried through? The controller should review implementation if there is a change in risk as a result of the processing.)*					

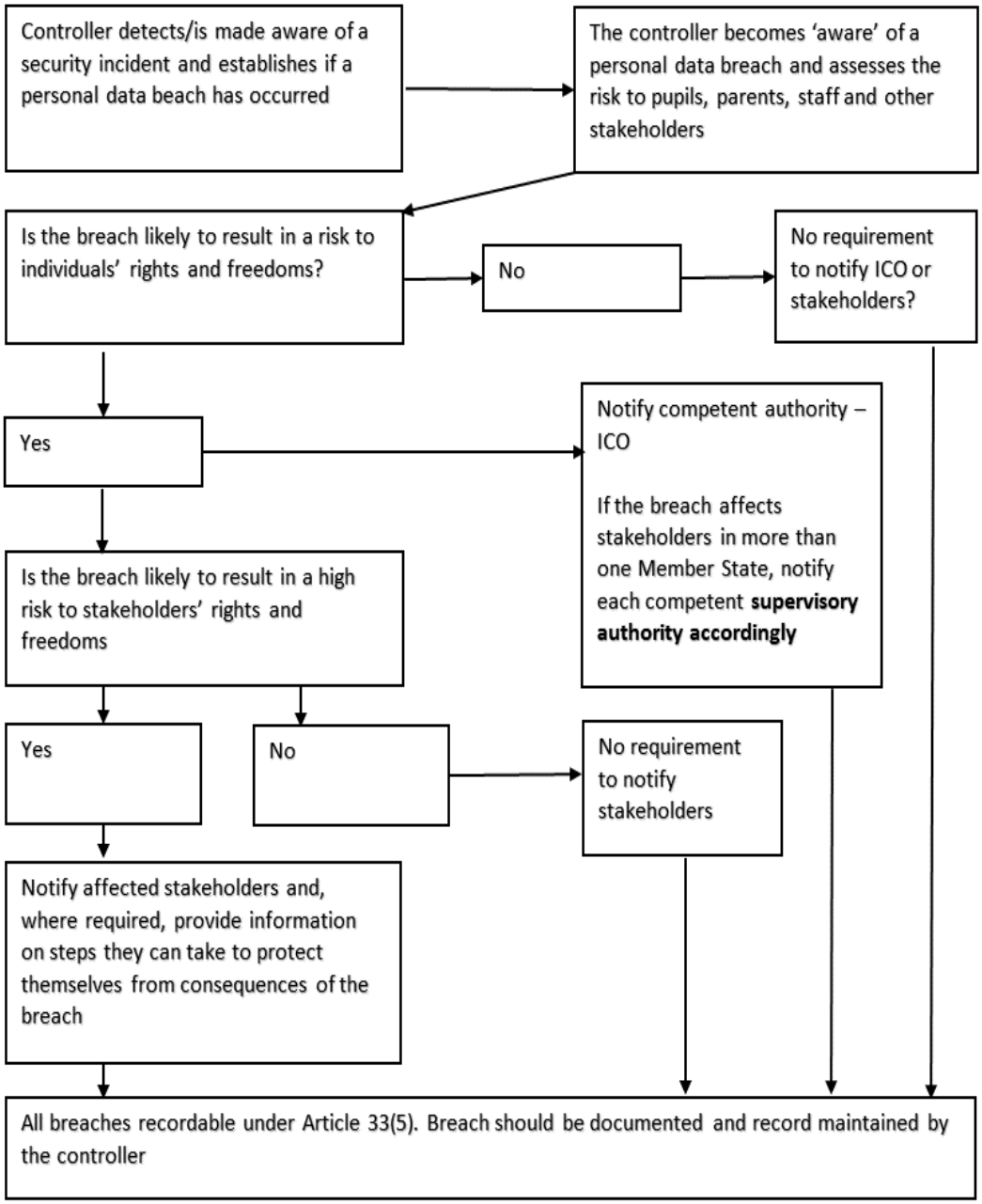
Conclusion


CONSEQUENCE
Catastrophic
Major
Moderate
Minor
Insignificant
5
4
3
2
1
5 10 15 20 25
4 8 12 16 20
3 6 9 12 15
2 4 6 8 10
1 2 3 4 5
1 2 3 4 5
Very unlikely
Unlikely
Fairly likely
Likely
Very likely
LIKELIHOOD
17-25 Unacceptable
Stop activity and make immediate improvements
10-16 Tolerable
Look to improve within specified timescale
5-9 Adequate
Look to improve at next review
1-4 Acceptable
No further action, but ensure controls are maintained

Annex C : Personal data breach procedure

Data Protection Officer (DPO) and reporting a data breach

A. Flowchart showing breach notification requirements – Heartlands Community Trust as Controller



B. Procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO

- The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people
- The DPO will alert the Chief Executive Officer, Head of School and the Chair of Directors
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
    - Loss of control over their data
    - Discrimination
    - Identify theft or fraud
    - Financial loss
    - Unauthorised reversal of pseudonymisation (for example, key-coding)
    - Damage to reputation
    - Loss of confidentiality
    - Any other significant economic or social disadvantage to the individual(s) concerned
- If it is likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.
- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the Google Drive
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:
    - A description of the nature of the personal data breach including, where possible:

        - The categories and approximate number of individuals concerned
        - The categories and approximate number of personal data records concerned
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned
- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - Facts and cause
    - Effects
    - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)
- Records of all breaches will be stored on the Google Drive
- The DPO, Chief Executive Officer and Head of School will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

Actions to minimise the impact of data breaches

The Trust will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. It will review the effectiveness of these actions and amend them as necessary after any data breach.

A. Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to recall it
- In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way
- The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request
- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted

Annex E : Breach Template

DPO/COMPLIANCE OFFICER/INVESTIGATOR DETAILS:			
NAME:		**POSITION:**	
DATE:		**TIME:**	
DDI:		**EMAIL:**	
INCIDENT INFORMATION:			
DATE/TIME OR PERIOD OF BREACH:			
DESCRIPTION & NATURE OF BREACH:			
TYPE OF BREACH:			
CATEGORIES OF DATA SUBJECTS AFFECTED:			
CATEGORIES OF PERSONAL DATA RECORDS CONCERNED:			
NO OF DATA SUBJECTS AFFECTED:		**NO OF RECORDS INVOLVED:**	
IMMEDIATE ACTION TAKEN TO CONTAIN/MITIGATE BREACH:			
STAFF INVOLVED IN BREACH:			
PROCEDURES INVOLVED IN BREACH:			
THIRD PARTIES INVOLVED IN BREACH:			
BREACH NOTIFICATIONS:			
WAS THE SUPERVISORY AUTHORITY NOTIFIED?			**YES/NO**
IF YES, WAS THIS WITHIN 72 HOURS?			**YES/NO/NA**

If no to the above, provide reason(s) for delay

IF APPLICABLE, WAS THE BELOW INFORMATION PROVIDED?	YES	NO
A description of the nature of the personal data breach		
The categories and approximate number of data subjects affected		
The categories and approximate number of personal data records concerned		
The name and contact details of the Data Protection Officer and/or any other relevant point of contact (for obtaining further information)		
A description of the likely consequences of the personal data breach		
A description of the measures taken or proposed to be taken to address the personal data breach (including measures to mitigate its possible adverse effects)		
WAS NOTIFICATION PROVIDED TO DATA SUBJECT?	**YES/NO**	

INVESTIGATION INFORMATION & OUTCOME ACTIONS:	
DETAILS OF INCIDENT INVESTIGATION:	
PROCEDURE/S REVISED DUE TO BREACH:	
STAFF TRAINING PROVIDED: *(if applicable)*	
DETAILS OF ACTIONS TAKEN AND INVESTIGATION OUTCOMES:	
HAVE THE MITIGATING ACTIONS PREVENTED THE BREACH FROM OCCURRING AGAIN? *(Describe)*	

WERE APPROPRIATE TECHNICAL PROTECTION MEASURES IN PLACE?	YES/NO
If yes to the above, describe measures	
Investigator Signature: _____ Date: _____ Investigator Name: _____ Authorised by: _____	