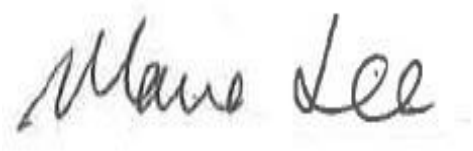
Young at Art Data Management Policy

Policy approved by Board/s on 24 June 2024

Policy Review Due Date: 24 June 2027

Signed by Chair as approved:



Maria Lee

Introduction

In the course of its business, Young at Art needs to gather and use certain information about individuals. These can include employees, contractors, customers, suppliers, business contacts, volunteers, audiences and potential audiences and other people we have a relationship with or may need to regularly contact.

This policy describes how this personal data must be collected, handled, stored and used to meet our data protection standards – and to comply with the law including the General Data Protection Regulations (GDPR).

This policy ensures Young at Art:

- Complies with data protection law and follows good practice;
- Protects the rights of our customers, staff and partners;
- Is transparent about how we store and process individuals' data; and
- Protects ourselves from the risks of a data breach

Responsibilities for Compliance

Overall responsibility for Young at Art's compliance with this policy and accompanying procedures will lie with the Young at Art Board. The day-to-day operational management will lie with Young at Art's Data Protection Officer.

Young at Art Data Protection Officer (DPO) will be the Young at Art's General Manager. As at the date of this policy, the Data Protection Officer is Kelly-Anne Collins. All queries, requests for access etc should be forwarded to the DPO at manager@youngatart.co.uk. The Young at Art Marketing Officer will assist the General Manager in this role. All departments will embed and monitor compliance within the scope of their role.

In particular, the DPO will:

- Keep the Young at Art Director and Board/s updated on data protection issues, risks and responsibilities;

- Document, maintain and develop this policy and related procedures in line with the schedule set out on the cover of this policy;
- Embed ongoing privacy measures into all our policies, projects and day-to-day activities including marketing and fundraising alongside the staff responsible for that project or activity;
- Disseminate this policy across the organisations, provide advice to staff and arrange regular training on data protection to ensure compliance is being adhered to;
- Be the first point of contact and manage ongoing subject access requests, deletion requests and queries from clients, stakeholders and data subjects about data protection related matters;
- Check and approve contracts or agreements with third parties that may handle Young at Art's sensitive data;

- Ensure all systems, services and equipment used for storing data meet acceptable security standards; and
- Ensure that regular checks and scans of security hardware and software are carried out to ensure they are functioning properly.

This policy applies to all staff, Board members, contractors and third party suppliers. All staff must be familiar with this policy and comply with its terms. All third party Data Processors Young at Art use to process data on its behalf must be GDPR compliant.

Scope of Personal Information processed

To ensure compliance with data protection law, Young at Art have undertaken a full audit of the data held by the organisations in order to ascertain the extent of the personal information including any sensitive special categories of personal information.

This information is laid out in our Data Controller Register. In this register, Young at Art sets out the following:

- Description of the data subjects;
- Description of the personal data;
- How the data has been collected;
- The purpose for which the data has been collected;

- The lawful basis under which the data has been collected;
- Any special conditions for processing special category data;
- Who the data is shared with;
- How long we will hold the data; and
- How the data is stored including any special measures to protection the security of that data.

Data Protection Principles

The Data Protection Act 2018 came into force in the UK on 25 May 2018. Young at Art will comply with the principles of data protection ('the Principles') enumerated in the law. We will make every effort possible in everything we do to comply with these principles.

1. <u>We will fairly and lawfully process personal data in a transparent way</u>

Young at Art will only collect data where lawful and where it is necessary for the legitimate purposes of Young at Art.

- The name and contact details of employees and contractors will be collected when they take up a position, and will be sued to contact them regarding administration related to their role.

Further information, including personal financial information and criminal records information may also be collected in specific circumstances where lawful and necessary (in order to process payments to the person or in order to carry out an Access NI check)

Lawful basis: Contract (the collection and use of data is fair and reasonable in relation to Young at Art completing tasks expected as part of working with the individuals;

- Any individual's name, contact details and other details may be collected at any time with their consent, in order for Young at Art to communicate to them about our projects and activities.

  Lawful basis: Consent

- Pseudonymous or anonymous data (including behavioural, technological and geographical/regional) on an individual may be collected via tracking 'cookies' when they access our website or interact with our emails, in order for us to monitor and improve our effectiveness on these channels.

  Lawful basis: Consent

2. <u>We only collect and use personal data for specific, explicit and legitimate purposes and will only use the data for those specified purposes.</u>

When collecting data, Young at Art will always provide a clear and specific privacy statement explaining why the data is required and what it will be used for.

3. <u>We will ensure any data collected is relevant and not excessive</u>

Young at Art will not collect or store more data than the minimum information required for its intended purpose.

4. <u>We will ensure that data is accurate and up to date</u>

Young at Art will ask employees to check and update their data on an annual basis. Any other individual data collected will be checked yearly and updated when new information has been given. Individuals will be able to update their data at any point by contacting the DPO.

5. <u>We will ensure that data is not kept longer than necessary</u>

Young at Art will keep records for no longer than is necessary to meet the intended use for which it was gathered (unless there is a legal requirement to keep records). The storage and intended use of data will be reviewed in line with Young at Art's data retention

policy. When the intended use is no longer applicable (eg. contact details for an employee who has left), the data will be deleted within a reasonable period.

6. We will keep personal data secure

Young at Art will ensure that data held by us is kept secure including:

- Electronically-held personal data will be held within a password protected and secure environment. Passwords should be changed regularly. Staff should use the password manager issued to create and store their passwords.
- Data will only be stored on an encrypted computer that is password protected.

- Passwords for electronic files will be re-set each time an individual with data access leave their role/position
- Physically-held personal data will be stored in a locked cupboard.
- Keys for locks securing physical data files should be collected by the DPO from any individual with access if they leave their role/position. The codes on combination locks should be changed each time an individual with data access leaves their role/position
- Access to data will only be given to relevant employees/contractors where it is clearly necessary for the running of a project. The DPO will decide in what situations this is applicable and will keep a master list of who has access to data.

7. Transfer to countries outside the EEA

Young at Art will not transfer data to countries outside the European Economic Area (EEA), unless the country has adequate protection for the individual's data privacy rights.

Individual's Rights

1. Right to be Informed

Whenever Young at Art collects data, it will provide a clear and specific privacy statement explaining why it is being collected and how it will be used.

Young at Art aims to ensure that individuals are aware that their data is being processed, and that they understand:

- Who is processing their data;
- What data is involved;
- The purpose for processing that data;
- The outcomes of data processing; and
- How to exercise their rights.

To that end, Young at Art have a privacy statement, setting out how data relating to these individuals is used by us.

The Young at Art privacy notice is attached to this policy as Appendix A.

2. Right of Access

Individuals can request to see the data Young at Art holds on them and confirmation of how it is being used.

Young at Art are supportive of the rights of individuals to request access to the personal information about them that may be held by our organisation/s. To facilitate this process, individuals are required to complete a Data Subject Access Request Form and return it to the DPO who will manage the request completion.

The Data Subject Access Request Form is attached to this policy as Appendix C.

Young at Art will comply with data protection law in regard to these requests including replying in writing to any data subject access requests within 30 calendar days confirming whether or not we hold any personal information about the applicant and either provide

the information requested or explain why it is not being provided. Where requests are complex or numerous, this may be extended to 60 calendar days.

Access requests will be recorded in a Data Subject Access Request Register. This Register will record the name of the Data Subject, the date of the request and the length of time that the request information will be held before deletion. In accordance with data protection law, information supplied in response to a request will be based on the data held at the date of receipt of the request.

All information held will be subject to routine or regular amendments or deletions as per data protection law current at the time or subject to our organisational reviews.

3. Right to Rectification

Individuals can request that their data be updated where it is inaccurate or incomplete. Young at Art will request that staff, Board members, volunteers and contractors check and update their data on an annual basis. Any requests for data to be updated will be processed within 30 calendar days.

4. Right to Object

Individuals can object to their data being used for a particular purpose. Young at Art will always provide a way for an individual to withdraw consent in all marketing communications. Where we receive a request to step using data, we will comply unless we have a lawful reason to use the data for legitimate interests or contractual obligation.

5. <u>Right to Erasure</u>

Following a data subject access request process has been undertaken, the individual may request verbally or in writing for a verification of the information held or a deletion. Young at Art will respond to the request within one month of receipt of request to delete.

Young at Art will consider the deletion of records where personal information:

- is no longer necessary for the purpose for which it was originally collected or processed it for;
- is held on the lawful basis of consent and the individual withdraws their consent;
- is held on the lawful basis of legitimate interest and the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing;
- is being processed for direct marketing purposes and the individual objects to that processing;
- has been processed; or

- must be deleted to comply with a legal obligation.

Where an application for deletion is manifestly unfounded or excessive, taking into account whether the request is repetitive in nature, Young at Art may refuse to comply with a request or consider requesting a reasonable fee based on the administrative costs of complying with the request. The reasons for making these decisions will be recorded and promptly provided to the applicant.

6. Right to Restrict Processing

Individuals can request that their personal data be 'restricted' – that is, retained and stored but not processed further (e.g. if they have contested the accuracy of any of their data, Young at Art will restrict the data while it is verified.)

Though unlikely to apply to the data processed by Young at Art, we will also ensure that rights related to portability and automated decision making (including profiling) are complied with where appropriate.

Ongoing documentation of measures to ensure compliance

Young at Art recognises that complying with data protection law is an ongoing process.

To ensure ongoing compliance, Young at Art will ensure that:

1. our Data Controller Register is kept up-to-date by:

    - conducting a yearly review across the organisation/s of data held and security/privacy measures in place; and

- update the document if and when new major new activities or projects are undertaken by us following any data protection impact assessment; and

2. ensure that all Young at Art core personnel take part in a yearly internal data protection review as well as internal top up training. For any new employees, Young at Art will source suitable data protection training. Young at Art will maintain records showing the training undertaken by employees on privacy and data protection matters.

To assist with making decisions regarding the legal retention of documents that contain personal information, Young at Art will follow the guidelines set out in its Data Retention Schedule. This is attached as Appendix D to this policy.

Where personal information is identified for destruction/deletion, Young at Art will undertake the following:

- Personal information stored in hard copy physically on the premises will be destroyed safely and securely, including shredding;
- Where personal information is stored in digital documents on digital devices held by employees, all reasonable and practical efforts will be made to remove data.

- Priority will be given to any instances where data is stored in active lists (e.g. where it could be used) and to sensitive data;
- Where deleting the data would mean deleting other data that we have a valid reason to keep (e.g. on old emails) then the data may be retained safely and securely but not used.

Data Protection Impact Assessments

Where required to by law, Young at Art will undertake a Data Protection Impact Assessments (DPIA) during the development phase of a new project/activity.

To ensure adherence to best practice and that privacy by design is an integral part of the development of new projects/activities, Young at Art will consider whether to carry out a DPIA where integral to the delivery of the project, Young at Art might be processing:

- sensitive data or data of a highly personal nature;
- data concerning vulnerable data subjects; and
- personal data in what amounts to a major new project for the organisation/s.

Where Young at Art decides not to conduct a DPIA in the above circumstances where they are not required to by law but it could be considered best practice to do so, Young at Art will note on a DPIA form when, how and why such a decision was made.

A Data Protection Impact Assessment form is attached to this policy as Appendix B.

Data Sharing

Young at Art Data Controller Register outlines the details of any/all third party organisations with whom we share personal information.

From time to time and being mindful of compliance with data protection law, Young at Art will enter into data sharing agreements with third parties. When doing so, Young at Art will ensure that such agreements detail the following matters:

- management of the collection of the necessary permissions;
- scope of the personal data to be shared including any meta-data that will be collected to enable the creation of an audit trail to support any responses to any data processing challenges or data subject access requests;
- security measures in place to protect the data in transit; and

- receiving organisations' obligations as a data controller of this new copy of the data being shared with them.

Security Measures

Young at Art collects, holds, processes and shares personal data, a valuable asset that needs to be suitably protected. Every care is taken to protect personal data from incidents (either accidentally or deliberately) to avoid a data protection breach that could compromise security.

Compromise of information, confidentiality integrity or availability may result in harm to individual(s), reputational damage, detrimental effect on service provision, legislative noncompliance and/or financial costs.

Young at Art is obliged under data protection law to have in place a framework designed to ensure the security of all personal data during its lifecycle, including clear lines of responsibility.

Young at Art's Data Controller Register outlines the details of all the security measures that we have in place to protect the personal information that we store from a data breach. It also sets out our protocols for the following:

1. Safe Transfer of Data
2. Password Management
3. Data Back Up

Young at Art will ensure that we have appropriate security measures in place to ascertain if there has been a breach of data and how serious that breach has been.

With regards to reporting breaches of data, Young at Art will abide by the reporting and notification requirements as set out by the Information Commissioner and Data Protection legislation.

Action to be taken in the event of a data Breach

On discovery of a data breach, the following actions should be taken:

1. Containment and Recovery

Immediate responsibility for taking action on discovery of the breach is the individual committing the breach and any staff, Board members, volunteers or contractors who become aware of the breach.

Their immediate priority should be to contain the breach and limit its scope and impact. Where personal data has been sent to or accessed by someone not authorised to see it, the individual aware of the breach should:

- Tell the recipient not to pass it on or discuss it with anyone else;
- Tell the recipient to destroy or delete the personal information they have received and get them to confirm in writing that they have done so;
- Warn the recipient of any implications if they further disclose the data; and
- Inform the data subjects whose personal data is involved what has happened so that they can take any necessary action to protect themselves.

The breach must be immediately reported to the DPO providing the following information:

- Date and time of the breach;
- Date and time the breach was detected;
- Who committed the breach;
- Details of the breach;
- Number of data subjects involved; and
- Details of actions already taken in relation to the containment and recovery.

See Appendix E for the reporting form to be used.

2. <u>Assessing the Risk</u>

Upon receiving a report of the breach of personal information, the DPO will conduct an investigation into the breach and prepare a report. The report will follow the Information Commissioner's Office guidance on breach management and will consider the following:

- How did the breach occur?;
- The type of personal data involved;
- The number of data subjects affected by the breach;
- Who the data subjects are;
- The sensitivity of the data breached;

- What harm to the data subjects can arise? For example, are there risks to physical safety, reputation or financial loss?;
- What could happen if the personal data is used inappropriately or illegally?;
- For personal data that has been lost or stolen, are there any protections in place such as encryption?; and
- Are there reputational risks from a loss of public confidence in the services that Young at Art?

3. Notifying the Information Commissioner's Office (ICO)

The DPO with advice from a Legal/Information Security Services will determine whether the breach is one which is required to be notified to the ICO. Where the decision is taken to notify the ICO, the DPO will complete a breach notification form.

4. Evaluation and Response

Following any breach, the DPO will review the circumstances surrounding the breach with those involved. Taking advice from Legal/Information Security Services, the DPO will implement appropriate changes to Young at Art's data management policies and

procedures to prevent further breaches. This may include additional staff training or information security measures.

APPENDIX A – YOUNG AT ART PRIVACY NOTICE

At Young at Art, we are committed to maintaining the trust and confidence of visitors to our website, subscribers to our newsletter, and those who purchase tickets for our events. Here you'll find information on how we treat data that we collect from visitors to our website, when someone subscribes to our newsletter, or when someone purchases tickets.

Visitors to our Website

When someone visits www.youngatart.co.uk we use a third-party service, Google Analytics, to collect standard internet log information and details of visitor behaviour patterns. We do this to find out things such as the number of visitors to the various parts of the site. This information is only processed in a way that does not identify anyone. We do

not make, and do not allow Google to make, any attempt to find out the identities of those visiting our website.

Newsletter Sign-Up

As part of the registration process for our monthly e-newsletter, we collect personal information (your email address, name, and postcode). We use that information for a couple of reasons: to tell you about what's happening at Young at Art, and occasionally other news from other organisations that we feel is of interest; to contact you if we need to obtain or provide additional information; to check our records are right, and to check

every now and then that you're happy and satisfied. We don't rent or trade email lists with other organisations and businesses.

We use a third-party provider, Mailerlite, to deliver our newsletter. We gather statistics around email opening and clicks using industry standard technologies to help us monitor and improve our e-newsletter. For more information, please see Mailerlite's Privacy Policy. You can unsubscribe to general mailings at any time of the day or night by clicking the unsubscribe link at the bottom of any of our newsletter emails or by emailing marketing@youngatart.co.uk.

Purchasing Tickets

When you purchase tickets or gift vouchers through our Box Office, your name, address, email, and contact number will be stored by our ticketing partner, Ticketsolve. When you purchase tickets, data is shared between Global Payments (payment gateway) and Ticketsolve (ticketing platform), in order to process the transaction. Where patrons opt to join the mailing list, data will be shared with Mailerlite (email partner).

Ticketsolve, Global Payments, and Mailerlite have implemented appropriate technological measures to protect against accidental loss, destruction, damage, alteration or disclosure of data. Global Payments is a trading name of GPUK LLP. GPUK LLP is authorised by the Financial Conduct Authority under the Payment Services Regulations

2017 (504290) for the provision of payment services and under the Consumer Credit Act (714439) for the undertaking of terminal rental agreements.

For more information, please see their privacy notices here:

- Ticketsolve
- Mailerlite
- Global Payments

Please be assured that we do not share your personal details with any other company without your consent. Where activity is delivered with a partner venue or organisation, we will provide them with a customer list (name and mobile number) in order to fulfil your booking and to be able to contact you in the event of any last minute changes. Partner venues or organisations are not allowed to store this beyond the event.

People who email us

We use Microsoft 365, which automatically encrypts email, turning them into a code during delivery. This security tool is called Transport Layer Security (TLS) and helps prevent others from reading our emails. If your email service does not support TLS, you should be aware that any emails we send or receive may not be protected in transit.

Microsoft also complies with the EU-U.S., UK Extension to the EU-U.S., and Swiss-U.S. Data Privacy Frameworks.

We will also monitor any emails sent to us, including file attachments, for viruses or malicious software. Please be aware that you have a responsibility to ensure that any email you send is within the bounds of the law.

Links to Other Websites

This privacy notice does not cover the links within this site linking to other websites. Those sites are not governed by this Privacy Policy, and if you have questions about how a site uses your information, you'll need to check that site's privacy statement.

Access to Your Personal Information

You are entitled to access the personal information that we hold. Email your request to the Data Protection Officer.

Changes to this Privacy Notice

We keep our privacy notice under regular review. This privacy notice was last updated on 24 June 2024.

Cookies Policy

We use a system of classifying the different types of cookies which we use on the Website, or which may be used by third parties through our website. The classification was developed by the International Chamber of Commerce UK and explains more about

which cookies we use, why we use them, and the functionality you will lose if you decide you don't want to have them on your device.

What is a cookie?

Cookies are text files containing small amounts of information which are downloaded to your personal computer, mobile or other device when you visit a website. Cookies are then sent back to the originating website on each subsequent visit, or to another website that recognises that cookie. Cookies are useful because they allow a website to recognise a user's device.

How long are cookies stored for?

Persistent cookies – these cookies remain on a user's device for the period of time specified in the cookie. They are activated each time that the user visits the website that created that particular cookie.

Session cookies – these cookies allow website operators to link the actions of a user during a browser session. A browser session starts when a user opens the browser window and finishes when they close the browser window. Session cookies are created temporarily. Once you close the browser, all session cookies are deleted.

Cookies do lots of different jobs, like letting you navigate between pages efficiently, remembering your preferences, and generally improve the user experience.

You can find more information about cookies

at www.allaboutcookies.org and www.youronlinechoices.eu.

Cookies used on our Website

A list of all the cookies used on our website by category is set out below.

Strictly necessary cookies

These cookies enable services you have specifically asked for. These cookies are essential in order to enable you to move around the website and use its features, such as accessing secure areas of the website.

Performance cookies

These cookies collect anonymous information on the pages visited. By using the website, you agree that we can place these types of cookies on your device.

These cookies collect information about how visitors use the website, for instance which pages visitors go to most often, and if they get error messages from web pages. These cookies don't collect information that identifies a visitor. All information these cookies collect is aggregated and therefore anonymous. It is only used to improve how the website works.

Functionality cookies

These cookies remember choices you make to improve your experience. By using the website, you agree that we can place these types of cookies on your device.

These cookies allow the website to remember choices you make (such as your username, language or the region you are in) and provide enhanced, more personal features. These

cookies can also be used to remember changes you have made to text size, fonts and other parts of web pages that you can customise. They may also be used to provide services you have asked for such as watching a video or commenting on a blog. The information these cookies collect may be anonymised and they cannot track your browsing activity on other websites.

Third party cookies

These cookies allow third parties to track the success of their application or customise the application for you. Because of how cookies work we cannot access these cookies, nor can the third parties access the data in cookies used on our site.

For example, if you choose to ‘share’ content through Twitter or other social networks you might be sent cookies from those websites. We don’t control the setting of these cookies, so please check those websites for more information about their cookies and how to manage them.

We embed videos from our official YouTube channel using YouTube’s privacy-enhanced mode. This mode may set cookies on your computer once you click on the YouTube video player, but YouTube will not store personally-identifiable cookie information for playbacks of embedded videos using the privacy-enhanced mode.

Read more at YouTube’s embedding videos information page.

APPENDIX B - DATA PROTECTION IMPACT ASSESSMENT FORM

Data Protection Impact Assessments form an integral part of a 'privacy by design', best practice approach. They are a tool which can help Young at Art identify the most effective way to comply with their data protection obligations and meet individuals'

expectations of privacy, and protect against the risk of harm through use or misuse of personal information.

Name of Staff Member	
Date of Assessment	
Project Title / Working Title	

Step 1 - Identify the Need for a DPIA				
Brief Project Description	Explain broadly what your project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal.			
Based on this description, is there a legal requirement on	Yes – If yes, you must		No	

us to conduct a DPIA? For details, see here - https://bit.ly/2mmucr5	complete a DPIA			
If no, do any of the following conditions apply: • sensitive data or data of a highly personal nature might be processed as	Yes		No	

an integral part of the project; • data concerning vulnerable data subjects might be processed as an integral part of the project; or • personal data might be processed as an integral part of the				

project and the project being considered is a major new development for the organisation.				
If no, please make a brief note of the reasons why your project does to meet any of these criteria.				

If yes, discuss with the Young at Art Data Protection Officer whether to proceed with completing a DPIA. A decision to proceed will depend on whether there is a likely high risk to the personal information being processed during the project.
Please note here the reasons for a decision not to proceed with a DPIA after discussions with your Data Protection Officer.
Step 2 - Describe the processing

Describe the nature of the processing involved in your project: How will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?
Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?
Step 3 - Consultation process
Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

Step 4 - Assess necessity and proportionality
Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

Step 5 - Identify and assess risks			
Describe source of risk and nature of potential impact on individuals.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
Include associated compliance and corporate risks as necessary	Remote, possible or probable	Minimal, significant or severe	Low, medium or high
Step 6 - Identify measures to reduce risk			

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5				
Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved**
		Eliminated reduced accepted	Low medium high	Yes/no
Step 7: Sign off and record outcomes				

Item	**Name/date**	**Notes**
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		If accepting any residual high risk, consult the ICO before going ahead

DPO advice provided:		DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice:		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		

Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will kept under review by:		The DPO should also review ongoing compliance with DPIA

APPENDIX C - DATA SUBJECT ACCESS REQUEST FORM

Subject access is one of the main rights under the Data Protection Act 2018. It gives you the right to ask us to tell you about any personal information that we might hold about you, and to provide you with a copy of that information. This is known as a data subject access request.

To submit a subject access request to Young at Art (*Circle which organisation/s your request relates*), please complete the below and return to our Data Protection Officer at manager@youngatart.co.uk or Cotton Court, 30-42 Waring Street, Belfast, BT1 2ED.

Once we receive a data subject access request, we must reply, in writing, within 40 calendar days. In our reply, we must confirm whether or not we hold any personal information and either provide the information requested or explain why it is not being provided.

Personal information about your child

Information about children may be released to a person with parental responsibility. However, the best interests of the children will always be considered. Before releasing any

information about children, Young at Art will undertake all reasonable measures to ensure that the applicant is a person with parental responsibility for the child.

Completing this form

Please be as clear and concise as possible, including, for example, providing your full name, any other names you are known by, and what areas of our activities you may have dealt with.

Title	
Full name of Applicant	
Former/Maiden Name or any other name by which you have been known	
Full name of person to whom this access	

request is made if it is on behalf of another person including a child	
Date of Birth	
Email Address	
Contact Phone Number	
Current Address	

Postcode	
What information are you requesting?	
Please provide any additional information that relates to your request	
Please attach your documentary proof of your identity	

You can prove your identity by providing at least two forms of identification that between them provide a combination of your name, current address, and date of birth. The documents that could be used for example might be a photocopy or scan of the photo identification page of your passport or driving licence, or a copy or scan of a current utilities bill or bank statement showing your current address. Do not send original documents as we cannot be held accountable for original documents lost in the post.

If you are making an access request on behalf of a child, please provide evidence of your parental responsibility for the child.

Would you like us to return this documentation? (Please indicate which applies)

Yes	
No, please destroy this documentation once you no longer need it	
How would you like us to correspond with you? (Please indicate which applies)	
By email, by using the email address provided above	
By post, using the address provided	

Your Declaration

The information that I have supplied in and attached to this access request form is correct and I am the person to whom it relates. I understand that if I am providing my signature electronically, it is legally enforceable.

Signature:		**Date:**	

A person who impersonates another or attempts to impersonate another may be guilty of an offence.

Our Data Protection Statement

Any personal information you give us will be held securely and in accordance with the rules on data protection. Your personal details will be treated as private and confidential and safeguarded, and will not be disclosed to anyone not connected to Young at Art depending on which organisation/s apply to you unless you have agreed to its release, or in certain circumstances where we are legally obliged to do so.

We will ensure that any disclosure made for this purpose is proportionate, considers your right to privacy and is dealt with fairly and lawfully in accordance with the Data Protection Principles of the Data Protection Act.

The Data Protection Act 2018 regulates the use of 'personal data', which is essentially any information, whether kept on computer or paper files, about identifiable individuals. As a 'data controller' under the Act, Young at Art must comply with its requirements.			
For Office Use Only – To be completed by the Data Protection Officer			
Receipted by: (Name)		**Date of Receipt:**	
How was the identity of the requester confirmed:			

APPENDIX D - YOUNG AT ART DOCUMENT RETENTION SCHEDULE

Young at Art will keep its documents and records depending on a number of factors including:

- Legal and related compliance requirements;

- Costs;
- Our needs to access the document; and
- Historical value.

Each document will be assessed separately.

Financial Records		
1. Purchase invoices and supplier documentation		
Document	**Retention Period**	**Reason for Retention Period**

Payments cash book or record of payments made	6 years from the end of the financial year in which the transaction was made	Companies Act / Charities Act
Purchase Ledger		Companies Act / Charities Act
Invoice – revenue		Companies Act / Charities Act
Petty cash records		Companies Act / Charities Act and HMRC
Invoice – capital item	10 years	Companies Act / Charities Act and HMRC

Successful quotations for capital expenditure	Permanently	Commercial considerations
2. Income/Monies received		
Document	**Retention Period**	**Reason for Retention Period**
Bank paying in counterfoils	6 years from the end of the financial year in which the transaction was made	Companies Act / Charities Act
Bank statements		Companies Act / Charities Act

Remittance advices		Companies Act / Charities Act
Correspondence re donations		Companies Act / Charities Act
Bank reconciliations		Companies Act / Charities Act
Receipts cash book		Companies Act / Charities Act and HMRC
Sales Ledger		Companies Act / Charities Act and HMRC

Deeds of covenant / Gift Aid declarations	6 years after the last payment was made. 12 years if payments outstanding or dispute regarding the deed.	Data Protection Act
Legacies	6 years after the estate has been wound up	Data Protection Act

3. Funding Grants		
Document	**Retention Period**	**Reason for Retention Period**
Relating to grants from the Arts Council of Northern Ireland	7 years	Terms & Conditions of Grant Offer
Tax Records		
Document	**Retention Period**	**Reason for Retention Period**

Transfer pricing documents and other records supporting the company's tax return	6 years after the end of the accounting period the tax return relates to / the date on which the enquiry period for the tax return closes	Finance Act
Records of all delivery of goods or services and of imports and exports for VAT purposes	6 years from the date the records were created	VAT Act 1994
Stamp Duty land tax documents	6 years from the effective date of the transaction /	Finance Act

	the date on which the tax enquiry into a return is completed or end of the period during which HMRC have power to make an enquiry into the return	
Payroll Documentation		
Document	**Retention Period**	**Reason for Retention Period**

Income tax records re employees leaving ie. P45	6 years plus current year	Taxes Management Act
Notice to employer of tax code (P6)		Taxes Management Act
Annual return of employees and directors expenses and benefits (P11D)		Taxes Management Act
Certificate of pay and tax deducted (P60)		Taxes Management Act
Notice of tax code change		Taxes Management Act

Annual return of taxable pay and tax deducted		Taxes Management Act
Record of pensions deductions (including superannuation)		Pensions Act
Clock cards / Timesheets	2 years after audit	Audit
Payroll and payroll control account	6 years plus current year	Companies Act / Charities Act and Taxes Management Act
Employee/personnel records		

Document	**Retention Period**	**Reason for Retention Period**
Medical records and details of biological tests under the control of Lead at Work Regulations	40 years from the date of the last entry	The Control of Lead at Work Regulations
Accident books, accident records/reports	3 years after last entry or end of investigation if later	The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995

Details of medical schemes	Permanently	Commercial
Organisation charts		Commercial
Personnel files and training records	Maximum 6 years after the employment ceased	Limitations Act 1980 and Data Protection Act
Wages and salary records	6 years plus the current year	Taxes Management Act
Expense accounts/records		Taxes Management Act
Overtime records/authorisation		Taxes Management Act
Redundancy details, calculations of payments,	6 years after employment has ceased	Data Protection Act

refunds, notifications to the Secretary of State		
Life Assurance expression of wish forms	6 years after employment ceases or death	Data Protection Act
Records relating to working time	2 years from the date on which they were made	The Working Time Regulations
Application forms and interview notes (for unsuccessful candidates) / Monitoring Forms (Check whether EQ has directions	6 months to a year	Disability Discrimination Act 1995 and Race Relations Act 1976 recommend 6 months. 1 year limitation

about keeping Monitoring Forms?)		for defamation actions under Limitations Act
Statutory Maternity Pay records, calculations, certificates or other medical evidence	3 years after the end of the tax year in which maternity period ends	The Statutory Maternity Pay Regulations
Statutory Sick Pay records, Calculations, certificates, self-certificates	3 years after the end of each tax year for Statutory Sick Pay purposes	Statutory Sick Pay (General) Regulations

National minimum wage records	3 years after the end of the pay reference period following the one that the records cover	National Minimum Wage Act
Records for key senior executives should be kept permanently for historical purposes		
Buildings, plant and engineering		
Document	**Retention Period**	**Reason for Retention Period**

Deeds of title	Permanently or until property is disposed of / Copies of title deeds should be kept for 6 years after disposal	Limitations Act 1980
Leases	12 years after the lease and liabilities under the lease have terminated	Limitations Act 1980
Records of major refurbishments, warranties, planning consents, design	13 years for actions against contractors etc	Limitations Act 1980

documents, final health and safety files		
Pension records		
Document	**Retention Period**	**Reason for Retention Period**
Details re current pensioners	10 years after benefit ceases	Commercial
Pension scheme – next of kin/expression of wish forms	6 years after date of death	Data Protection Act

All trust deeds and rules	Permanently	Companies Act / Commercial / Pensions Act
Trustees' minute book		Companies Act / Commercial / Pensions Act
Annual accounts		Companies Act / Commercial / Pensions Act
Pension scheme investment policies	12 years from the ending of any benefit payable	Companies Act / Commercial / Pensions Act
Actuarial reports	Permanently	Companies Act / Commercial / Pensions Act

Contribution records		Companies Act / Commercial / Pensions Act
Insurance documents		
Document	**Retention Period**	**Reason for Retention Period**
Policies	3 years after lapse	Data Protection Act
Claims correspondence	3 years after settlement	Data Protection Act
Employers Liability insurance certificate	40 year	Employers' Liability (Compulsory Insurance) Regulations 1998

Accident reports and relevant correspondence	3 years after settlement	Data Protection Act
Other documents		
Document	**Retention Period**	**Reason for Retention Period**
Trustee / Director / Governor minutes of meetings and decisions made as resolutions in writing	Minimum 10 years from the date of the meeting or from the date of passing a resolution in writing	Data Protection Act / Companies Act / Charities Act

Minutes of general meetings and members' resolutions passed other than at a general meeting	Minimum 10 years after the date of the meeting / resolution / decision	Companies Act / Charities Act
Annual accounts and annual review	Permanently	Data Protection Act
Major agreements of historical significance		Data Protection Act
Health & Safety records	3 years for general records. Permanently for records	Personal injury actions must generally be commenced within 3 years of injury.

	relating to hazardous substances	However, industrial injuries not capable of detection within that period (e.g. Asbestos) the time period may be substantially extended.
Fixed assets register	Permanently	Companies Act / Charities Act / Commercial
Contract with customers, suppliers or agents, licensing agreements, rental/hire	6 years after expiry or termination of the contract. If the contract is	Limitations Act 1980

purchase agreements, indemnities and guarantees and other agreements or contracts	executed as a deed, the limitation period is 12 years	(6 years is generally the time limit within which proceedings founded on contract may be brought. Actions for latent damages may be brought up to 15 years after the damage occurs)
All other documents (eg. contact lists, photographs) will be held subject data protection legislation and will be reviewed on an annual basis. These documents are held for commercial and archival purposes.		

APPENDIX E – DATA BREACH REPORTING FORM

To help the Young at Art Data Protection Officer manage any breaches of personal information held by the organisations, please complete the following form as fully as possible upon becoming aware of a data security breach.

Once completed, return the form to the Young at Art DPO.

Name	
Title/Role	

Date/Time Breach Occurred	
Who committed the breach	

Details of the breach	

Number of Data Subjects **involved**	

Details of actions taken to contain breach/recover personal information	