Artish Huddersfield CIC

DATA PROTECTION POLICY

Policy Created: 20th March 2023

Table of Contents

Statement of intent..... 3

Equal opportunities and inclusion 3

1. Aims..... 4
2. Scope of the Policy 4
3. Definitions of data protection terms 5
4. Roles and Responsibilities..... 6
5. Personal Data Protection Principles..... 7
6. Lawfulness, Fairness and Transparency..... 9
7. Sharing personal data..... 9
8. Consent 10
9. Subject access requests and other rights of individuals..... 11
10. CCTV 12
11. Photographs and videos..... 12
12. Protection of Biometric information..... 13
13. Record keeping..... 14
14. Accountability, data protection by design 14
15. 15 Data security and storage of records..... 14
16. 16 Retention schedule 16
17. 17 Destruction of records 17
18. 18 Disclosure and Barring Service (DBS) data..... 17
19. 19 Personal data breaches..... 17
20. 20 Training..... 17
21. 21 Review and Monitoring arrangements..... 18
22. Appendix A..... 18

Statement of intent

Artish Huddersfield CIC is required to keep and process certain information about its staff members and pupils in accordance with its legal obligations under the UK General Data Protection Regulation (UK GDPR) and Data Protection Act (DPA) 2018

Artish Huddersfield CIC may, from time to time, be required to share personal information about its staff or pupils with other organisations, mainly the LA, other schools and educational bodies, and potentially children's services.

This policy is in place to ensure all Directors are aware of their responsibilities and outlines how **Artish Huddersfield CIC** complies with the following core principles of the UK GDPR.

Organisational methods for keeping data secure are imperative. **Artish Huddersfield CIC** believes that it is good practice to keep clear practical policies, backed up by written procedures.

This policy complies with the requirements set out in the UK GDPR.

Equal opportunities and inclusion

It is the right of all children, staff and visitors to **Artish Huddersfield CIC**, regardless of their gender, ethnicity, religion or beliefs, physical disability, ability, linguistic, cultural or home background, to have their personal information collected, stored and processed in line with the requirements of the current legislation.

Links to UN Rights of the Child:

Article 13

Every child must be free to say what they think and to seek and receive all kinds of information as long as it is within the law.

Article 17

Every child has the right to reliable information from the media. This should be information that children can understand. Governments must help protect children from materials that could harm them.

1 Aims

Artish Huddersfield CIC uses personal information about staff, pupils, parents/carers/guardians and other individuals who come into contact with the organisation. This information is gathered, in order to enable it to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that **Artish Huddersfield CIC** complies with its statutory obligations.

Artish Huddersfield CIC has a legal responsibility to comply with data protection legislation and other statutory provisions relating to the way in which it holds and processes personal data. **Artish Huddersfield CIC** as a corporate body, is named as the data controller under the Data Protection Act 2018 (DPA 2018).

ICO Notification and Registration. **Artish Huddersfield CIC** is required to 'notify' the Information Commissioner of the processing of personal data. This information is included in a public register which is available on the Information Commissioner's website. As a Data controller **Artish Huddersfield CIC** will register annually with the ICO as required in line with legislation.

Privacy Notices. All Company Directors, contractors, and partners of **Artish Huddersfield CIC** that hold its' personal information, has to comply with the law when managing that information. We have a duty to issue a

privacy notice to all pupils, parents/carers/guardians and volunteers/employees; these provide details of information collected and held, why it is held and the other parties to whom it may be passed on.

Data Controller. As data controller personal data collected about staff, pupils, parents/carers/guardians, visitors and other individuals that is collected and held must be processed in accordance with the UK General Data Protection Regulation (UK GDPR) and the DPA 2018.

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

This policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the Data Protection Act 2018 and the UK GDPR. It will apply to information regardless of the way it is used, recorded, stored and whether it is held in paper files or electronically.

2 Scope of the Policy

We recognise that the correct and lawful treatment of personal data will maintain confidence in **Artish Huddersfield CIC**. Protecting the confidentiality and integrity of Personal Data is a critical responsibility that we take seriously at all times. Under the UK GDPR, personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

This includes any expression of opinion about an individual and intentions towards an individual. It also applies to personal data held visually in photographs or video clips (including CCTV) or as sound recordings.

Artish Huddersfield CIC collects a large amount of personal data every year including: staff records, names and addresses of those requesting references, fee collection as well as the many different types of research data used by Artish Huddersfield CIC In addition, it may be required by law to collect and use certain types of information to comply with statutory obligations of Local Authorities (LAs), government agencies and other bodies.

3 Definitions of data protection terms

Consent: agreement which must be freely given, specific, informed and be an unambiguous indication of the data subject's wishes by which they, by a statement or by a clear positive action, signifies agreement to the processing of personal data relating to them.

Data controllers: are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with the Act. We are the data controller of all personal data used in our organisation for our own operational purposes.

Data Privacy Impact Assessment (DPIA): tools and assessments used to identify and reduce risks of a data processing activity. DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or business change programs involving the Processing of Personal Data.

Data processors: include any person or organisation that is not a data user who processes personal data on our behalf and on our instructions. Employees of data controllers are excluded from this definition, but it could include suppliers which handle personal data on ARTISH Huddersfield CIC behalf.

Data Protection Officer (DPO): is the individual or organisation appointed by Artish Huddersfield CIC to be, responsible for monitoring our compliance with data protection law.

Data subject: means a living, identified or identifiable individual about whom we hold personal data. Data subjects may be nationals or residents of any country and may have legal rights regarding their personal data.

Data users: are those of our employees whose work involves processing personal data. Data users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times.

Personal data: means any information relating to an identified or identifiable natural person (data subject). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Personal data breach: any act or omission that compromises the security, confidentiality, integrity or availability of personal data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of personal data is a personal data breach.

Processing: is any activity which is performed on personal data such as collection, recording, organisation, structuring, adaptation or alteration, using, storage, retrieval, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Special category personal data: includes information about a person's racial or ethnic origin, political opinions; religious or philosophical beliefs; trade union membership; physical or mental health or condition; genetic/biometric data held for purposes of identification or data about sexual orientation or an individual's sex life.

4 Roles and Responsibilities

This policy applies to all personal data we process regardless of the media on which that data is stored or whether it relates to past or present pupils, employees, workers, or supplier contacts, website users or any other data subject.

Staff, those working on our behalf and volunteers

This policy applies to all staff employed by **Artish Huddersfield CIC**, and to external organisations or individuals working on our behalf.

You must read, understand and comply when processing personal data on our behalf and attend training on its requirements. This policy sets out what we expect from you, in order for **Artish Huddersfield CIC** to comply with applicable law. Your compliance with this policy is mandatory. You must also comply with all related policies and guidelines given. Staff who do not comply with this policy may face disciplinary action.

All staff are responsible for:

- ➢ Collecting, storing and processing any personal data in accordance with this policy
- ➢ Ensuring that personal data held is accurate and up to date
- ➢ Ensuring that personal data held is not misused, lost or unlawfully disclose

The DPO is Karen Marsden who can be contacted at artishcic@gmail.com

All staff must contact the Data Protection Officer in the following circumstances:

- Where they are unsure or have questions about the operation of this policy; the purposes for which data may be used; retaining personal data; disclosing personal data or keeping personal data secure
- If there has been a data breach or a suspected data breach
- Where they are unsure if they have a lawful basis for processing personal data or wish to process for a different purpose than the one that the data was obtained
- Where they propose to engage in any activity that affects the rights of privacy of any individual i.e. where there is a legal obligation to carry out a DPIA
- Where they are unsure about what security, or other measures they need to implement to protect personal data
- If they are engaging in an activity that may affect the privacy rights of individuals
- If they need any assistance dealing with any rights invoked by a data subject
- Where they are considering sharing personal data with third parties
- Where they are entering into contracts involving the processing of personal data by another organisation
- If they need to transfer personal data outside the European Economic Area

Where staff have concerns that this policy is not being followed by others, they should report this immediately to the DPO. Where they wish to raise this formally, they may do so under the **Artish Huddersfield CIC** whistleblowing policy for staff.

Governing Board

The Directors have overall responsibility for ensuring compliance with all relevant data protection obligations. All policies and documents related to data protection are reviewed annually.

Data Protection Officer

The 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. They will provide an annual report of their activities at the AGM and where relevant, report their advice and recommendations on **Artish Huddersfield CIC** data protection issues. The DPO is also a point of contact for individuals whose data **Artish Huddersfield CIC** processes, who wish to raise any complaint regarding Artish Huddersfield CIC processing where they remain dissatisfied with the company's response, and for the Information Commissioner's Office (ICO).

5 Personal Data Protection Principles

Artish Huddersfield CIC adheres to the principles relating to processing of personal data set out in the UK GDPR which require personal data to be:

a. processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency')
b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('purpose limitation');
c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

d. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
e. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the UK GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation');
f. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

Artish Huddersfield CIC is responsible for and must be able to demonstrate compliance with the data protection principles listed above (Accountability). Making available to data subjects and data subjects allowed to exercise certain rights in relation to their personal data (Data Subject's Rights and Requests).

Artish Huddersfield CIC is committed to maintaining the data protection principles at all times. This means that **Artish Huddersfield CIC** will:

- Inform data subjects, via privacy notices about the processing of their personal data. Who is it collected by, how is it being used and Who is it shared with.
- Check the quality and accuracy of the information held
- Apply the records management policies and procedures to ensure that information is not held longer than is necessary
- Ensure that when information is authorised for disposal it is done appropriately • Ensure appropriate security measures are in place to safeguard personal information whether that is held in paper files or on a computer system
- Only share personal information with others when it is necessary and legally appropriate to do so
- Set out clear procedures for responding to requests for access to personal information known as subject access request
- Train all staff so that they are aware of their responsibilities and of Artish Huddersfield CIC relevant policies and procedures

6 Lawfulness, Fairness and Transparency

Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject. **Artish Huddersfield CIC** may only collect, process and share Personal Data fairly and lawfully and for specified purposes. The UK GDPR restricts our actions regarding personal data to specified lawful purposes. These restrictions are not intended to prevent processing, but ensure that we process personal data fairly and without adversely affecting the data subject.

The UK GDPR allows processing for specific purposes, some of which are set out below:t

a. the data subject has given his or her consent;
b. the processing is necessary for the performance of a contract with the data subject;
c. to meet our legal compliance obligations.;
d. to protect the data subject's vital interests;
e. the data needs to be processed so that Artish Huddersfield CIC as a public authority, can perform a task in the public interest, and carry out its official functions - this is known as the public task

f. to pursue our legitimate interests for purposes where they are not overridden because the processing prejudices the interests or fundamental rights and freedoms of data subjects.

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the UK GDPR and DPA 2018.

If **Artish Huddersfield CIC** offers online services to pupils, such as classroom apps, and we intend to rely on public task, legal obligation and or consent as a basis for processing we will obtain parental consent as necessary (except for online counselling and preventive services).

When we collect personal data directly from data subjects, including for human resources or employment purposes, we provide the data subject with all the information required by the UK GDPR, including the identity of the Data Controller and DPO, how and why we will use, process, disclose, protect and retain that personal data through a fair processing (privacy) notice.

7 Sharing personal data

- **Artish Huddersfield CIC** will not normally share personal data with anyone else without express consent, but may do so where:
- It is necessary for the performance of our public task
- There is an issue with a pupil or parent/carer/guardian that puts the safety of another individual at risk
- For safeguarding purposes

Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we:

- Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
- Establish either in the contract or as a standalone agreement, a data processing agreement to ensure the fair and lawful processing of any personal data we 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

Artish Huddersfield CIC will also share personal data with law enforcement and government bodies where we are legally required to do so, including for the following purposes:

- 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

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff and for safeguarding purposes.

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

Artish Huddersfield CIC may enter into information-specific sharing agreements with other public bodies for the

purposes outlined above.

8 Consent

Consent will be sought prior to processing any data which cannot be done so under any other lawful basis, such as complying with a regulatory requirement.

Consent must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes.

Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes.

Where consent is given, a record will be kept documenting how and when consent was given.

Artish Huddersfield CIC ensures that consent mechanisms meet the standards of the UK GDPR. Where the standard of consent cannot be met, an alternative legal basis for processing the data must be found, or the processing must cease.

Consent accepted under the DPA will be reviewed to ensure it meets the standards of the UK GDPR; however, acceptable consent obtained under the DPA will not be reobtained.

Consent can be withdrawn by the individual at any time.

Where a child is under the age of 13, the consent of parents/carers/guardians will be sought prior to the processing of special categories of their data, except for safeguarding to prevent harm and where the processing is related to preventative or counselling services offered directly to a child.

When gaining pupil consent, consideration will be given to the age, maturity and mental capacity of the pupil in question. Consent will only be gained from pupils where it is deemed that the pupil has a sound understanding of what they are consenting to.

9 Subject access requests and other rights of individuals

Our data subjects have rights when it comes to how we handle their personal data. These include rights to:

- withdraw consent to processing at any time;
- receive certain information about how we process their data;
- Request access to their personal data that we hold.
- prevent the use of their personal data for direct marketing purposes;
- Ask us to erase personal data if it is no longer necessary in relation to the purposes for which it was collected or processed or to rectify inaccurate data or to complete incomplete data.
- Restrict processing in specific circumstances;
- challenge processing, which has been justified on the basis of our legitimate interests or in the public interest;
- request a copy of an agreement under which personal data is transferred outside of the EEA; • object to decisions based solely on automated processing, including profiling (known as automated decision making ('ADM'));
- prevent processing that is likely to cause damage or distress to the data subject or anyone else;
- be notified of a personal data breach which is likely to result in high risk to their rights and freedoms; and
- make a complaint to the Information Commissioner.

How to make a subject access request

The UK GDPR does not specify how to make a valid request.

You can make a subject access request verbally or in writing to any part of Artish Huddersfield CIC and not a specific contact point. We suggest however that you email **Artish Huddersfield CIC** if possible:

We have one month to respond to your request.

UK GDPR requests for personal data are free in most cases unless the request is manifestly unfounded or excessive, when a "reasonable fee" for the administrative costs of complying with the request may be charged.

A reasonable fee will be charged based on administrative costs if an individual requests further copies of their data following a request.

When responding to requests, **Artish Huddersfield CIC** may ask the individual to provide 2 forms of identification and contact the individual to confirm that they made a request.

We may inform the requester that **Artish Huddersfield CIC** will comply within 3 months of receipt of the request, where a request is complex or numerous requests have been made, informing the requester of this within 1 month, and explaining why the extension is necessary.

Artish Huddersfield CIC will not disclose information if by doing so it:

- ➢ might cause serious harm to the physical or mental health of the pupil 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.

When **Artish Huddersfield CIC** refuses a request, the individual will be advised of the reason and that they have the right to complain to the ICO.

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/carers/guardians of pupils at **Artish Huddersfield CIC** may not be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

Parents, or those with parental responsibility, have a legal right to access to their child's record (which includes most information about a pupil) within 15 days of receipt of a written request.

11 Photographs and videos

As part of **Artish Huddersfield CIC** activities, we may take photographs and record images of individuals within our venues.
Artish Huddersfield CIC will obtain consent from parents/carers/guardians for the general use categories of photos and videos.

Artish Huddersfield CIC will obtain written consent from parents/carers/guardians for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both

the parent/carer/guardian and pupil. Where we don't need parental consent, we will clearly explain to the pupil how the photograph and/or video will be used.

Marketing and promotional materials uses may include:

- on notice boards and in **Artish Huddersfield CIC** magazines, brochures, prospectuses newsletters, etc.
- Outside of **Artish Huddersfield CIC** by external agencies such as the **Artish Huddersfield CIC** photographer, newspapers, campaigns
- Online on our website or social media pages

When using photographs and videos in this way **Artish Huddersfield CIC** will not include any other personal information about the child, to ensure they cannot be identified, unless parent/carer/guardian consent is provided, and safeguarding is not compromised.

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

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

12 Protection of Biometric information

Legal Framework:

Protection of Freedoms Act 2012, Data Protection Act 2018, UK GDPR and DfE guidance 'Protection of biometric information of children in schools and colleges'

At **Artish Huddersfield CIC**, the written consent of at least one parent/carer/guardian must be obtained before the biometric data is taken from the child and used. This applies to all pupils in schools and colleges under the age of 18.

In no circumstances can a child's biometric data be processed without written consent. We will not process the biometric data of a pupil (under 18 years of age) where:

a. the child (whether verbally or non-verbally) objects or refuses to participate in the processing of their biometric data;
b. no parent/carer/guardian has consented in writing to the processing; or
c. a parent/carer/guardian has objected in writing to such processing, even if another parent/carer/guardian has given written consent.

We will where possible provide reasonable alternative means of accessing services for those pupils who will not be using an automated recognition system.

We refer to the latest guidance published by the DfE for the implementation of policy https://www.gov.uk/government/publications/protection-of-biometric-information-of-children-in schools

13 Record keeping

UK GDPR requires us to keep full and accurate records of all our data processing activities.

We keep and maintain accurate records reflecting our processing. These records include clear descriptions of the personal data types, data subject types, processing activities, processing purposes, third-party recipients of the

personal data, personal data storage locations, personal data transfers, the personal data's retention period and a description of the security measures in place.

14 Accountability, data protection by design

Artish Huddersfield CIC put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO
- 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
- Completing data protection impact assessments where **Artish Huddersfield CIC** 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)
- 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; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant

15 Data security and storage of records

We 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 and consider:

Network security - The ICT company and or technician will ensure that network security is effectively operating and updating.

Software updates (patch management) – The ICT company and or technician will ensure effective patch management, to minimise vulnerabilities.

Malware protection – Antivirus and anti-malware software will be installed to prevent, malware, which is intentionally designed to cause damage to a computer, server, client, or computer network.

Access control – Access to systems will be minimised and be based on the need and requirement of users.

Firewalls – A firewall that monitors and controls incoming and outgoing network traffic, based on predetermined security rules. Will be installed at all times to establish a barrier between Artish Huddersfield CIC's trusted network and the internet (untrusted network).

Secure configuration - Secure configuration will be adopted when installing computers and network devices, to reduce the risk of cyber threats.

Data Protection Impact Assessments - DPIA's will be undertaken to systematically analyse, identify and minimise the data protection risks of a project or plan

Web filtering - Web filtering will be employed at all times (content control software)

Staff training - Cyber security including, phishing attacks, ransomware and awareness of further training, from the National Cyber Security Centre.

Practical measures include and are not limited to:

- Passwords that are at least 8 characters long where possible containing letters and numbers are used to access 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, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for equipment
- Where Artish CIC needs to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and is adequately protected
- Confidential paper records will be kept in a locked filing cabinet, locked cupboard, drawer or safe, with restricted access.
- Confidential paper records will not be left unattended or in clear view anywhere with general access.
- Digital data is coded, encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed up off site.
- Where data is saved on removable storage or a portable device, the device will be kept in a locked filing cabinet, drawer or safe when not in use.
- Memory sticks will not be used to hold personal information unless they are password protected and fully encrypted. Staff are provided with encrypted memory stick by Artish Huddersfield CIC as necessary.
- All electronic devices are password-protected to protect the information on the device in case of theft.
- Where possible, Artish CIC enables electronic devices to allow the remote blocking or deletion of data in case of theft.
- Staff will not use their personal laptops or computers for Artish CIC purposes if it involves the identifiable data of pupils, staff member or any other stake holder.
- All necessary members of staff are provided with their own secure login and password, and every computer regularly prompts users to change their password.
- Emails containing sensitive or confidential information are password-protected if there are unsecure servers between the sender and the recipient.
- Circular emails to parents/carers/guardians, are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.
- Where personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, staff will take extra care to follow the same procedures for security, e.g. keeping devices under lock and key. The person taking the information accepts full responsibility for the security of the data.

Before sharing data, all staff members will ensure:

- They are allowed to share it.
- That adequate security is in place to protect it.
- Who will receive the data.
- They will check if unsure.

Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas containing sensitive information are supervised at all times.

The physical security of storage systems, and access to them, is reviewed on a regular basis. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place.

Artish CIC takes its duties under the UK GDPR seriously, and any unauthorised disclosure may result in disciplinary action.

Artish Huddersfield CIC is responsible for continuity and recovery measures are in place to ensure the security of protected data.

Storage of records

Artish CIC has a responsibility to maintain its records and record keeping systems. When doing this, will take account of the following factors: -

- The most efficient and effective way of storing records and information;
- The confidential nature of the records and information stored;
- The security of the record systems used;
- Privacy and disclosure; and
- Their accessibility.

16 Retention schedule

Approved Information (hard copy and electronic) will be retained for at least the period specified in the retention schedule. When managing records, Artish CIC will adhere to the standard retention times listed within that schedule. Paper and Electronic records will be regularly monitored by the directors. The retention periods are based on business needs and legal requirements.

17 Destruction of records

Where records have been identified for destruction, they should be disposed of in an appropriate way. All information must be reviewed before destruction to determine whether there are special factors that mean destruction should be delayed, such as potential litigation, complaints or grievances.

We will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on Artish Huddersfield CIC's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

.

18 Disclosure and Barring Service (DBS) data

All data provided by the DBS will be handled in line with data protection legislation; this includes electronic communication. Data provided by the DBS will never be duplicated. Any third parties who access DBS information will be made aware of the data protection legislation, as well as their responsibilities as a data handler.

19 Personal data breaches

Artish Huddersfield CIC will make all reasonable endeavours to ensure that there are no personal data breaches. A personal data breach is more than just losing personal data. It is a breach of security leading to the accidental or lawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity

or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on individuals.

In the event of a suspected data breach, we will follow the Artish Huddersfield CICs Personal Data Breach Procedure (see Appendix A) and take all steps we can to remedy the breach that has occurred.

When appropriate, we will report the data breach to the ICO within 72 hours.

20 Training

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

Data protection will also form part of continuing professional development, where changes to legislation, guidance or Artish Huddersfield CIC processes make it necessary.

17

21 Review and Monitoring arrangements

This policy is reviewed at least annually by the Companies Directors and the Data Protection Officer (DPO).

For help or advice on this policy and further specialist information may be sought from Artish CIC please contact the Data Protection Officer at artishcic@gmail.com

This policy is reviewed and ratified by Directors and the DPO.

_____

Appendix A

Data Breach Procedure

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

On finding or causing a breach, or potential breach, or a breach that is likely to have occurred. The staff member or data processor must immediately notify the DPO (Data Protection Officer).

The DPO will decide if there are any conflicts of interest and, if there are, the relevant person will step away from the process.

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 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)

18

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's 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 Artish Huddersfield CIC computer system. 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
- 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 securely. The DPO will review what happened and how it can be stopped from happening again. This review will occur as soon as reasonably possible.

Actions to minimise the impact of data breaches

In the event of a data breach, Artish Huddersfield CIC will take action to mitigate the impact of the breach, particularly if it involves sensitive information. Artish Huddersfield CIC will review the effectiveness of these actions and amend them as necessary after any data breach.

Signed:  Dated: 20th March 2023

Name (please print): D P Barker

Position in organisation: Director

Review Date:

- ➢ March 2024 - No changes
- ➢ March 2025 - No changes
- ➢ March 2026 - No changes
- ➢ March 2027 -
- ➢ March 2028 -