Data Protection Policy

Title	Data Protection Policy
Date of update	28/08/2025
Date of approval	30/09/2025
Approved by	innov8 Workshops CIO Trustees
Date of next review	August 2026

Table of contents

1. Executive summary

1.1. This policy outlines the principles of the Data Protection Act 2018 (DPA 2018) and the General Data Protection Regulations (GDPR) and identifies how innov8 Workshops complies with the DPA 2018 and GDPR. It aims to give guidance on how the requirements of the DPA 2018 and GDPR apply to the work of innov8 Workshops.

1.2. This policy covers all personal data that innov8 Workshops holds in either electronic or paper format and applies throughout the life cycle of the data from the time it is created or arrives within innov8 Workshops, to the time it is either destroyed or permanently preserved.

1.3. This policy applies equally to all innov8 Workshops' employees, Board members, Trustees, agency staff and contractors.

1.4. This policy also identifies responsibilities for data protection, and gives more specific guidance on the following areas:

1.4.1. Notification to the Information Commissioner

1.4.2. Special Categories of Data (sensitive personal data)

1.4.3. Staff records and monitoring

1.4.4. Use of CCTV

1.4.5. Retention and disposal of personal data

1.4.6. Data subject access requests

1.4.7. Disclosure of data to third parties

1.4.8. Privacy notices

1.4.9. Data breach

1.4.10. Training and awareness

1.4.11. Security.

1.5. Further guidance is available on the Information Commissioner's Office website.

2. Context

2.1. GDPR balances the legitimate needs of organisations to store and use personal data with the rights of individuals who are the subject of this data. If an organisation collects or holds information about an identifiable natural person, or if it uses, discloses, retains or destroys that information, it is likely to be processing personal data.

2.2. GDPR is underpinned by a set of six straightforward, common-sense principles which, if followed, will ensure compliance with GDPR. GDPR also requires that 'the controller shall be responsible for; and be able

to demonstrate compliance with the principles' – this is referred to as accountability. These principles are set out at 3.2 below.

2.3. Compliance with GDPR is monitored and enforced by the Information Commissioner's Office (ICO). The ICO has the power to impose sanctions, including fines of up to £17 million for a serious breach of one or more of the six principles and where the breach is likely to cause substantial damage or distress. The ICO can also impose additional fines of up to £8.5 million for breaches of an organisation's governance procedure (accountability). This is in addition to any penalties imposed by the courts against individuals who unlawfully breach GDPR or violate Article 8 of the Human Rights Act – The Right to Privacy.

2.4. GDPR uses many terms which have a specific meaning in the context of these regulations, and therefore a glossary of these terms is included at the end of this policy.

2.5. innov8 Workshops collects and uses certain types of data about people, in order to continue to provide the level of service expected by its users, customers, partners and counterparties and to comply with the requirements of local government. This data includes personal details about current, past and prospective employees, suppliers, funders, partners and others with whom we communicate.

2.6. As an organisation which deals with personal data innov8 Workshops will ensure it:

2.6.1. complies with both the law and best practice.

2.6.2. respects the rights of individuals.

2.6.3. is open and honest with individuals whose data is held.

2.6.4. provide support and training for those who handle personal data, so that they can act confidentially and consistently.

3. Achieving compliance with the DPA 2018 and GDPR – principles

3.1. The main purpose of the six principles of GDPR is to protect the interests of individuals whose personal data is being processed (that is information or data obtained, recorded or held, or the carrying out of any

operation or set of operations on the information or data). They apply to everything innov8Workshop does with personal data, except where an exemption applies. The key to complying with GDPR is to follow the six principles relating to the processing of personal data.

3.2. Below is a summary of the six principles and the ways in which innov8 Workshops complies with them.

3.3. The first principle states that personal data shall be processed lawfully, fairly and in a transparent manner (lawfulness, fairness and transparency) and in particular, shall not be processed unless:

3.3.1. at least one of the conditions in Article 6 of GDPR is met; and

3.3.2. in the case of special categories of personal data (sensitive), at least one of the conditions in Article 9 of GDPR is also met.

3.4. In practice, this means innov8 Workshops must:

3.4.1. have legitimate grounds for collecting and using the personal data.

3.4.2. not use the data in ways that have unjustified adverse effects on the individuals concerned.

3.4.3. be transparent about how they intend to use the data and give individuals appropriate privacy notices when collecting their personal data.

3.4.4. handle people's personal data only in ways they would reasonably expect.

3.4.5. make sure they do not do anything unlawful with the data.

3.5. We do this by:

3.5.1. abiding by the law in all activities

3.5.2. ensuring data subjects are aware of how their data will be used at the time they provide it and not using it for any purpose incompatible with the original stated purpose.

3.5.3. ensuring the data has been provided by a person who is legally authorised, or required, to provide it.

3.5.4. ensuring that the processing of personal data meets one of the legitimising conditions listed in Article 9 of GDPR

3.5.5. ensuring that all processing of personal data meets one of the following conditions:

3.5.5.1. The data subject gives consent for one or more specific purposes.

3.5.5.2. The processing is necessary to meet contractual obligations entered into by the data subject.

3.5.5.3. The processing is necessary to comply with the legal obligations of the controller.

3.5.5.4. The processing is necessary to meet the vital interests of the data subject.

3.5.5.5. The processing is necessary for tasks in the public interest, or an exercise of authority vested in the controller.

3.5.5.6. The purposes of legitimate interests pursued by the controller.

3.6. Further conditions are in place for special categories of personal data, see section seven for further guidance.

3.7. **The second principle** states that personal data shall be 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 purpose (purpose of processing).

3.8. In practice this means that we must:

3.8.1. be clear ('explicit') from the outset about why we are collecting personal data and what we intend to do with it

3.8.2. comply with Article 13 of GDPR requirements – including the duty to provide privacy notices to individuals at the point of collecting their personal data

3.8.3. ensure that if the council wishes to use or disclose the personal data for any purpose that is additional to or different from the original specified purpose, the new use is compatible with the original specified purpose.

3.9. We do this by:

3.9.1. At the time data is obtained the data subject will be informed of the purpose for which the data is being collected. Purposes may be specified in a privacy notice given in accordance with Article 13 requirements.

3.10. **The third principle** states that personal data shall be adequate, relevant and limited to what is necessary in relation to the purpose for which it is processed (data minimisation).

3.11. In practice this means:

3.11.1. data must be the minimum necessary for fulfilling the purpose for which it is processed.

3.11.2. innov8 Workshops does not collect information it does not need.

3.11.3. the data must be adequate for need.

3.12. We do this by:

3.12.1. collecting only the minimum amount of personal data required to fulfil the processing needs, or to comply with legal requirements. Additional unnecessary data will not be collected, and data will not be held on the off chance that it might be useful in the future.

3.13. **The fourth principle** states that personal data must be accurate and where necessary, kept up to date (accuracy).

3.14. We do this by:

3.14.1. taking reasonable steps to ensure the accuracy of any personal data obtained; ensure that the source of any personal data is clear; carefully consider any challenges to the accuracy of the information; consider whether it is necessary to update the information.

3.15. **The fifth principle** states that personal data should be kept in a form which permits identification for no longer than is necessary for the purposes for which the personal data are processed (retention).

3.16. In practice this means we will need to:

3.16.1. review the length of time we may lawfully keep personal data.

3.16.2. consider the legitimacy of purpose or purposes for which innov8 Workshops hold information in deciding whether (and for how long) to retain it.

3.16.3. securely delete information that we are not holding lawfully or legitimately.

3.16.4. update, archive or securely delete information if it goes out of date.

3.17. We will do this by:

3.17.1. only holding personal data as long as it is necessary for the lawful processing purpose for which it has been provided/obtained.

3.17.2. if personal data is collected for a specific project, it shall be disposed of as soon as the project comes to an end.

3.17.3. complying with our record retention guidance.

3.18. **The sixth principle** states that personal data should be processed in a manner that ensures appropriate security of the personal data (security).

3.19. In practice this means we will need to:

3.19.1. ensure a level of security appropriate to the nature of the data and harm that might result from a breach of security.

3.19.2. design and organise security to fit the nature of the personal data held and the harm that may result from a security breach.

3.19.3. be ready to respond to any security incident swiftly and effectively.

3.19.4. be sure there is the right physical and technical security, backed up by robust policies and procedures and reliable well-trained staff.

3.19.5. be clear about who in the organisation is responsible for organising information security.

3.20. We will do this by ensuring we have robust technical and organisational security measures including (amongst others):

3.20.1. Password protection of computer systems

3.20.2. Controlled access to innov8 Workshops buildings

3.20.3. Access rights of users appropriate to the needs of their job.

3.20.4. Management to ensure that performance, regarding personal data, is regularly assessed and evaluated.

3.20.5. All staff to have a level of understanding of the DPA 2018 and GDPR commensurate with their duties.

3.20.6. Adequate checks to ensure the suitability of all staff who have access to personal data.

3.20.7. Management to ensure that everyone managing, and handling data is subject to appropriate line management.

4. Record of processing activities

4.1. innov8 Workshops maintains a record of processing activities capturing much of the above, including:

a. the condition relied upon for the processing.

b. how the processing satisfies Article 6 and 9 of GDPR, and

c. whether the personal data is retained and erased in accordance with innov8 Workshops' Document Retention Guidance.

5. Roles and responsibilities

Data controller

5.1. For the purpose of the DPA 2018 and GDPR the data controller is innov8 Workshops.

Senior Information Risk Officer – Daniela Symons

5.2. innov8 Workshops Senior Information Risk Officer (SIRO) with specific responsibility for managing information risks is the Head of Provision of innov8 Workshops – Daniela Symons.

Data Protection Officer – School's Choice data.protection@schoolschoice.org

5.4. innov8 Workshops' Data Protection Officer with specific responsibility to ensure that innov8 Workshops is compliant with the DPA is School's Choice.

Information Governance Officer – Daniela Symons

5.5. The Information Governance Officer will act as a link officer between the mentors and the Data Protection Officer when there is an issue relating to data protection, to:

5.5.1. Advise the Data Protection Officer if a data subject access request has been received in any workshop and support the mentor in drawing up its response.

5.5.2. Maintain a data or privacy breach notification procedure and register, and assist the Data Protection Officer in reviewing breaches, why they arose and potential system improvements which may be required.

5.5.3. Review the various application forms used within innov8 Workshops to ensure they include the reasons why innov8 Workshops needs to collect and store the personal information requested, and how they will use this information (privacy notices)

5.5.4. Determine the extent to which personal information is shared with others and whom it is shared with (internally and externally)

5.5.5. Conduct a regular review of the types of personal data being processed by innov8 Workshops, reporting any changes to the Data Protection Officer and ensuring compliance is maintained.

5.5.6. Maintain a training and awareness programme.

5.5.7. Support services in undertaking Data Protection Impact Assessments

Mentors

5.6. Mentors have responsibility for ensuring that their workshop complies with the principles of DPA 2018 and GDPR when processing personal data. This includes ensuring that all are aware of their responsibilities under data protection and trained to discharge those responsibilities.

Staff

5.7. All staff have a responsibility to ensure that they comply fully with DPA 2018 and GDPR. It is a criminal offence to knowingly or recklessly obtain or disclose personal data. They should not process any personal

data unless they are sure they are authorised to do so. Staff failing to comply with this policy could be subject to action under innov8 Workshops' disciplinary procedure.

6. Notification

6.1. The ICO maintains a public register of data controllers. DPA 2018 and GDPR requires every data controller, who is processing personal data, to notify and review their notification, on an annual basis.

6.2. It is an offence under data protection legislation if the notification is not kept up-to date, and an offence to use personal data in a manner which has not been notified.

6.3. It is the responsibility of all Mentors to advise the Information Governance Officer of any changes to the use of personal data within their workshops as soon as they occur so that innov8 Workshops' notification can be updated.

6.4. innov8 Workshops' notification will be reviewed annually and kept up to date by the Data Protection Officer.

7. Special categories of personal data (sensitive)

7.1. Extra care must be taken when processing special categories of personal data as additional requirements under DPA 2018 and GDPR must be met to ensure that the processing is legitimate and safe. At least one of the legitimising conditions described under Article 6, and also one of the legitimising conditions (Article 9) shown below, must be met.

7.2. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

7.3. Paragraph 7.2 shall not apply if one of the following applies:

7.3.1. the data subject has given explicit consent.

7.3.2. processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law.

7.3.3. processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving consent.

7.3.4. processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not- for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects

7.3.5. processing relates to personal data which are manifestly made public by the data subject.

7.3.6. processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.

7.3.7. processing is necessary for reasons of substantial public interest, which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

7.3.8. processing is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems.

7.3.9. processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy.

7.3.10. processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1).

7.4. innov8 Workshops has an Appropriate Policy Document regarding the use of conditions and the advice of the Data Protection Officer should be sought before the processing or collection of special category personal data for any new purpose commences.

8. Staff records and the monitoring of staff

8.1. innov8 Workshops should comply with the ICO's 'Employment Practices Code' in relation to the processing of staff personal data. This code is intended to help employers comply with the DPA and to encourage them to adopt good practice. The code aims to strike a balance between the legitimate expectations of staff that personal data about them will be handled properly and the legitimate interests of employers in deciding how best, within the law, to run their own organisations carrying out their legitimate business.

8.2. In particular, staff monitoring should only be carried out in accordance with this code. A copy of the code is available on the ICO website – Employment Practice Code.

9. CCTV monitoring

9.1. CCTV monitoring must only be carried out in accordance with the ICO's guidance. A copy of this is available on the ICO website. It is important that we respect people's privacy and uphold their rights, listen carefully to any Staff concerns and ensure that there is a clear and proportionate reason for using CCTV. Before CCTV can be used on innov8Workshop premises, the decision to deploy will need to be approved by the Board with clear recorded reasons for using it. This will include a Data Protection Risk Assessment (DPIA). innov8 Workshops also has a separate CCTV policy.

10. Retention and disposal of personal data

10.1. It is the responsibility of innov8 Workshops to hold personal data and to ensure that the data they hold is kept accurate and up to date and is not held for any longer than is necessary for the purpose for which it was collected.

10.2. When the data is no longer required, innov8 Workshops must dispose of the data safely. Guidance on retention periods for classes of data is set out in innov8 Workshops' Record Management Guidance.

10.3 All documents will be stored for a minimum of 7 years unless the data protection officer specifies a different time scale. Please refer to our Record Management Guidance.

11. Data Subject Access Requests (DSARs)

11.1. It is one of the fundamental rights of the individual under GDPR to be able to access their information. Individuals have the right to obtain:

11.1.1. confirmation that their data is being processed.

11.1.2. access to their personal data

11.1.3. other supplementary information – this largely corresponds to the information that should be provided in a privacy notice.

11.2. It is in the interests of innov8 Workshops to have an open and honest approach with all individuals on which they hold data.

11.3. The DPA 2018 and GDPR sets out guidance and a time limit within which a DSAR must be answered.

11.4. Any individual requesting access to their personal data is asked to complete a request in writing which must be referred to the Data Protection Officer. This gives clarity around the date the request was made and therefore the deadline date and also encourages the individual to think clearly about the data they require. However, under data protection legislation, personal data requests do not have to be made in writing, a verbal request is just as legitimate; guidance regarding DSARs is available on innov8 Workshops' website and includes access to a DSAR application form.

11.5. The individual making the request must produce a document such as a passport or driving licence to confirm his identity.

11.6. innov8 Workshops will approach all requests for data in an open and honest way and seek to ensure that the individual gets all the data they require as long as this is permissible within the law.

11.7. There will be some requests where it will not be possible or appropriate to release personal data, for example, when doing so would involve releasing personal data about another individual, or if the data relates to ongoing criminal investigations. There may also be occasions when we cannot comply with specific requests regarding other aspects of the rights of the data subject, for example when dealing with GDPR Article 17 the Right to Erasure. This shall not apply to the extent that processing is necessary for compliance with a legal obligation which requires processing by law to which the controller is subject or for the

performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. Any concerns about releasing data should be discussed with the Data Protection Officer prior to release of the information.

11.8. More information on the procedure for recognising and responding to a DSAR can be found on the Intranet: How to – General Data Protection Regulation and Data Protection Act 2018 - Data Subject Access Request.

12. The right to be informed and privacy notices

12.1. The right to be informed encompasses innov8 Workshops' obligation to provide fair processing information, typically through a privacy notice. It emphasises the need for transparency over how we use personal data.

12.2. The information supplied in the privacy notice is determined by whether or not the personal data was obtained directly or indirectly from the individual.

12.3. The information innov8 Workshops supplies about the processing of personal data must be:

12.3.1. concise, transparent, and easily accessible

12.3.2. written in clear and plain language, particularly if addressed to a child.
12.3.3. free of charge

12.4. Further guidance on how to comply with 'the right to be informed' is provided in the: ICO Privacy Notice Code of Practice 13.

13. Sharing personal data

13.1. Where requests are received from external organisations or third parties for personal data about individuals, advice should be sought from the Data Protection Officer unless there is an up-to-date information-sharing or data exchange agreement in place with that organisation or third party. Under no circumstances should any personal data about any individual be passed outside innov8 Workshops without the authority of the Data Protection Officer unless an approved data sharing agreement is in place. More information can be found on the Intranet: General Data Protection Regulation and Data Protection Act 2018 - Third party requests. Where an officer considers information about a child or young person must be disclosed to a third party under the safeguarding provisions they must do so in accordance with innov8 Workshops Safeguarding Policy.

13.2. Agencies which request data on a regular basis such as the police or banks will have easy access to appropriate paperwork and guidance for use in these circumstances.

13.3. It should be noted that whilst staff understandably will wish to assist external agencies wherever possible especially if the request relates to criminal activity (for example the police or banks), innov8 Workshops is under no obligation to release personal data unless the request is made by a court order.

13.4. Personal data should generally only be made public if there is a legal or statutory requirement to do so for example under an exemption. On occasions it may be appropriate to publish personal data with the individual's consent. However, in such cases staff must ensure consent is 'freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her'. Staff must also be aware that it is possible to withdraw consent at any time and, if that happens, publication of the data must cease immediately.

13.5. Staff should be aware that publishing personal data on innov8 Workshops' website or on the internet by any other means effectively means that the data is published world-wide and outside the European Economic Area. This means it cannot be protected by the DPA 2018 and GDPR or the European Directive on Personal Privacy. Great care should be taken before publishing any personal data (or any data from which individuals could be identified) in this manner and the approval of innov8 Workshops' Data Protection Officer and Senior Information Risk Owner should be obtained before publication.

14. What to do in the event of a data breach

14.1. The ICO defines a data breach as a 'breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provisions of a public electronic communications service.

14.2. A personal data breach includes but is not restricted to the following:

14.2.1. The accidental alteration or deletion of personal data.

14.2.2. The transfer of personal data to those who are not entitled to receive it.

14.2.3. Unauthorised access to personal data.

14.2.4. Use of personal data for purposes for which it has not been collected and which go beyond those uses that the data subject could not have reasonably contemplated.

14.2.5. Theft of storage devices.

14.3. If a member of staff becomes aware of a data breach their first action should be to inform their line manager, who will then ensure that the breach is reported to the Data Protection Officer.

14.4. The Data Protection Officer will then decide on the most appropriate steps to take depending on the nature and quantity of data released. An investigation will be conducted into all data breaches.

14.5. The ICO will be informed of all serious data breaches where significant harm to an individual(s) is likely or a large number of individuals are affected.

14.6. More information on reporting personal data breaches can be found as follows: General Data Protection Regulation and Data Protection Act 2018 - Personal data breach.

15. Training and awareness

15.1. In order to fully comply with the DPA 2018 and GDPR it is important that all staff who have access to any personal data have an awareness of the regulations.

15.2. Training is a crucial element of staff awareness. innov8 Workshops' staff must be aware of their obligations relating to personal data as part their duties.

15.3. Training may be achieved in a number of ways:

15.3.1. all staff to be made aware of this Data Protection Policy

15.3.2. e-learning tools, and

15.3.3. in-house training provided by the Data Protection Officer

15.4. For some posts additional training and guidance is required. Those posts will be identified through their work and any additional training and guidance will need to be discussed with the line manager in the first instance.

16. Keeping information secure

16.1. The Sixth Principle of GDPR requires organisations to take appropriate technical and organisational measures to keep data secure. The security of data held by innov8 Workshops is a key priority and more information on the technical details of information security can be found in the innov8 Workshops Information Security Policy.

16.2. However, security of data goes beyond the use of computer equipment. Data will inevitably be stored or processed in hard copy forms at some time and access to this must be restricted to only those authorised to view it. As a general guide hard paper copies should not be left in the open in offices but should be kept locked away when not in use, in the same way as computer terminals should not be left unlocked and unattended.

16.3. It is important to remember that individuals should only be able to access data which they need to do their job. Personal data should not be left unattended and freely available to anyone in the office.

Working from home

16.4. When working from home, employees must ensure they only use their encrypted laptops to access personal data electronically. Paper files which include personal information must be kept in secure cases (lockable) at all times when not in use.

16.5. Under no circumstances should hard copy files be left unattended.

17. Administration

17.1. The Data Protection Officer has overall responsibility for the maintenance and operation of this policy and will be pleased to answer any questions about it.

17.2. Responsibility for monitoring adherence to this policy belongs with the Information Governance Officer.

17.3. This policy will be reviewed at least every year by the Board to confirm it reflects best practice and to ensure it complies with any legislative changes or amendments. Any significant and necessary changes will be made by the Senior Information Risk Officer and the Data Protection Officer.

Appendix A - GUIDANCE FOR STAFF

Responsibilities of Individual Data Users

All employees of innov8 Workshops who record/process personal data must ensure that they comply with the requirements of the GDPR. Any personal data should be kept securely. Personal data must not be disclosed verbally or in writing or otherwise to any unauthorised third party.

A breach of the GDPR or innov8 Workshops Data Protection Policy may result in disciplinary proceedings. Contact the Data Protection Officer for advice when unsure.

Authorised employees

Staff should only have access to personal data in the following circumstances:

- If they are assigned as mentor for that specific young person
- For personnel/HR issues, where the employee is authorised to access personnel files.
- Where the employee is authorised to access personal data in specific circumstances e.g. legal cases and complaints
- Service auditors
- Investigating officers
- Finance team

Employees must not access student records with whom they are not directly involved nor the HR records of people they know without legitimate reason for doing so.

Telephones

Staff should

- Not make phone calls concerning confidential information where you can be overheard by other students and visitors to the workshop.
- Be aware that some people may attempt to glean information to which they are not entitled. Staff are encouraged to check that they are speaking to the correct person by verifying the date of birth of the student involved or by calling back a number that can be checked independently. If staff suspect a caller is fake they must not release any information and report the incident to the Data Protection Officer

Email

When email is used to send sensitive information staff should

- Mark the email as 'Confidential'
- Where possible students should be referred to by first and last initial

- Always double check to ensure the email address is correct.
- Ensure emails containing sensitive information to external organisations are encrypted by clicking Options – Encrypt on Outlook.

Social Media

innov8 Workshops will at times use social media to show case the work of our students and mentors, during the recruitment process and to promote our services. Staff are reminded to consider the potential impact on confidentiality, their own reputation and that of innov8

Workshops as an organisation. Staff are expected to behave responsibly, professionally and in accordance with the innov8 Workshops Staff Code of Conduct.

Staff must not:

- Make unkind personal comments about colleagues or innov8 Workshops CIO.
- Be pictured in activities or make comments that may be open to misinterpretation.
- Engage in any activities that could bring innov8 Workshops into disrepute.
- Use their own mobile devices when taking photos of children for reporting and publicity purposes. Any student who is photographed must have given their consent for this by completing the innov8 Workshops 'GDPR Permission Form'. Permission can be granted by the school/provision/parent or guardian of the student.

Post

Staff are requested to ensure that:

- If correspondence contains any information that identifies a person, it is marked 'Private and Confidential' and is in a sealed envelope.
- Ensure that post is sent to a named person.
- If the correspondence contains significant amounts of information that identifies a student, it should be sent by Recorded Delivery
- Special Delivery should be used for extremely sensitive information.

Photography and Filming

innov8 Workshops has a duty of care to protect our students whose confidentiality may be at risk of being breached.

Casual photography or filming is not permitted in any public areas at innov8 Workshops sites. innov8 Workshops staff are permitted to take photographs for media purposes with the appropriate consent. Consent can be recorded through completion of the innov8 Workshops 'GDPR

Permission Form'. Permission can be granted by the school/educational provider/parent or guardian of the student.

Students and visitors attending the sites of innov8 Workshops must be informed (and if required reminded) that the filming and photography of persons and people is prohibited without the consent of the person being recorded. In situations where a student or visitor does not comply with this guidance, they will be asked to cease using their device.

Any incident where a student or visitor has been recorded without consent should be reported to the Data Protection Officer and a record should be made of the incident. The incident needs to be documented including details of the actions taken.

Confidential Waste

Any confidential paper waste must be shredded.

Cyber Security

Do:

- Set a strong password
- Lock computers and workstations when not in use
- store digital devices securely when not in use

Don't:

- Share passwords
- Use your own device for personal use
- Allow unauthorised staff, friends or relatives to use your work provided device

Text Messages

Text messages should not normally be used to convey sensitive information and use of text messages for the transfer of personal data should be kept to a minimum.

Sharing Information with other organisations

Care must be taken to ensure that disclosures are not made inadvertently and that those receiving the information in a professional capacity also have obligations to maintain confidentiality. Only

information that it is necessary to share should be shared and when information is shared it should be clear that the information should only be used for the purpose for which it was shared.

Information Sharing Agreements

Data Sharing Agreements are stated in innov8 Workshop SLA's which must be signed by both parties.

Retention of Data

Data protection law requires that 'Personal data shall be 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' is any information relating to a living individual who can be identified, directly or indirectly from it, in particular by reference to a name, location data or an online identifier. As part of its commitment to the GDPR, innov8 Workshops commits to storing data securely for the minimal length of time necessary.

Staff Training, Support and Monitoring

As part of the mandatory training schedule all staff at innov8 Workshops are required to complete GDPR training annually. It is the responsibility of the individual member of staff to complete up to date records of having completed GDPR training. Support is available from the Data Protection Officer. Compliance with GDPR training will be evidence through annual performance reviews.

Data Subject Access

Any individual may make a subject access request at any time to find out more about the personal data which innov8 Workshops holds about them. innov8 Workshops is normally required to respond to subject access requests within one month of receipt (this can be extended by up to two months in the case of complex and/or numerous requests and in such cases the individual concerned shall be informed of the need for extension).

All subject access requests received must be forwarded to innov8 Workshops CIO Data Controller. The Data Controller can be contacted on the details below:

Daniela Symons

daniela@innov8workshops.com
Tel: 07442 860088
innov8 Workshops
INTEG House
Woodlands Business Park
Rougham Industrial Estate
Bury St Edmunds
Suffolk
IP30 9ND

Data Portability

Individuals have the right to receive the personal data concerning him or her which he or she has provided to the data controller in a structured, commonly used and machine-readable format and have the right to transmit that data to another controller without hindrance from the controller to which the personal data has been provided.

Erasure of Personal Data

Individuals may request that innov8 Workshops CIO erases the personal data it holds about them in the following circumstances:

- It is no longer necessary for innov8 Workshops CIO to hold that personal data with respect to the purpose for which it was originally collected or processed.
- The individual now objects to innov8 Workshops CIO holding and processing their personal data.
- The personal data has been processed unlawfully.
- The personal data needs to be erased for innov8 Workshops to comply with a particular legal obligation

Unless innov8 Workshops has reasonable grounds to refuse all requests, erasure shall be complied with and the data subject informed of the process of erasure being completed.

Appendix B

ARTICLE 6 GDPR

Lawfulness of Processing

1. Processing shall be lawful only if and to the extent that at least one of the following applies:

    1. the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

    2. processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

    3. processing is necessary for compliance with a legal obligation to which the controller is subject;

    4. processing is necessary in order to protect the vital interests of the data subject or of another natural person;

    5. processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

    6. processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such

interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.

2. Member States may maintain or introduce more specific provisions to adapt the application of the rules of this Regulation with regard to processing for compliance with points (c) and (e) of paragraph 1 by determining more precisely specific requirements for the processing and other measures to ensure lawful and fair processing including for other specific processing situations as provided for in Chapter IX.
3. [1]The basis for the processing referred to in point (c) and (e) of paragraph 1 shall be laid down by:

    1. Union law; or

    2. Member State law to which the controller is subject.

    [2]The purpose of the processing shall be determined in that legal basis or, as regards the processing referred to in point (e) of paragraph 1, shall be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. [3]That legal basis may contain specific provisions to adapt the application of rules of this Regulation, inter alia: the general conditions governing the lawfulness of processing by the controller; the types of data which are subject to the processing; the data subjects concerned; the entities to, and the purposes for which, the personal data may be disclosed; the purpose limitation; storage periods; and processing operations and processing procedures, including measures to ensure lawful and fair processing such as those for other specific processing situations as provided for in Chapter IX. [4]The Union or the Member State law shall meet an objective of public interest and be proportionate to the legitimate aim pursued.
4. Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to

ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia:

1. any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;

2. the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;

3. the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10;

4. the possible consequences of the intended further processing for data subjects;

5. the existence of appropriate safeguards, which may include encryption or pseudonymisation.

Appendix C

ARTICLE 9 GDPR

Processing of special categories of personal data

1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

2. Paragraph 1 shall not apply if one of the following applies:

    1. the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

2. processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

3. processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

4. processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

5. processing relates to personal data which are manifestly made public by the data subject;

6. processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

7. processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

8. processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

9. processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

10. processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

3. Personal data referred to in paragraph 1 may be processed for the purposes referred to in point (h) of paragraph 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies.

4. Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health.

Appendix D – GDPR glossary of terms

For the purposes of this regulation:

1. ***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.

2***. processing*** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

3. ***restriction of processing*** means the marking of stored personal data with the aim of limiting their processing in the future.

4. ***profiling*** means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

5. ***pseudonymisation*** means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

6. ***filing system*** means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

7. ***controller*** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

8. ***processor*** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

9. ***recipient*** means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.

10. ***third party*** means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

11. ***consent of the data subject*** means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

12. ***personal data breach*** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

13. ***genetic data*** means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.

14. ***biometric data*** means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.

15. ***data concerning health*** means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status

16. ***main establishment*** means: a. as regards a controller with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment b. as regards a processor with establishments in more than one Member State, the place of its central administration in the Union, or, if the processor has no central administration in the Union, the establishment of the processor in the Union where the main processing activities in the context of the activities of an establishment of the processor take place to the extent that the processor is subject to specific obligations under this regulation.

17. *representative* means a natural or legal person established in the Union who, designated by the controller or processor in writing pursuant to Article 27, represents the controller or processor with regard to their respective obligations under this regulation.

18. ***enterprise*** means a natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity.

19***. group of undertakings*** means a controlling undertaking and its controlled undertakings.

20. ***binding corporate rules*** means personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity.

21. ***supervisory authority*** means an independent public authority which is established by a Member State pursuant to Article 51.

22. ***supervisory authority concerned*** means a supervisory authority which is concerned by the processing of personal data because: a. the controller or processor is established on the territory of the Member State of that supervisory authority b. data subjects residing in the Member State of that supervisory authority are substantially affected by the processing, or c. a complaint has been lodged with that supervisory authority.

23. ***cross-border processing*** means either: a. processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one member state, or b. processing of personal data which takes place in the context of the activities of a single establishment of

a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State

24. ***relevant and reasoned objection*** means an objection to a draft decision as to whether there is an infringement of this Regulation, or whether envisaged action in relation to the controller or processor complies with this Regulation, which clearly demonstrates the significance of the risks posed by the draft decision as regards the fundamental rights and freedoms of data subjects and, where applicable, the free flow of personal data within the Union

25. ***information society service*** means a service as defined in point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council(1) 26. international organisation means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries.