PLAYBACK

Data Protection Policy

Playback Studio collects and uses personal information (referred to in the Data Protection Act as personal data) about staff, clients and other individuals who come into contact with the centre. This information is gathered in order to enable the provision of educational support and other associated functions. In addition, the centre may be required by law to collect, use and share certain information.

Playback studio is registered as a Data Controller, with the Information Commissioner's Office (ICO). Details are available on the ICO website. https://ico.org.uk

Playback Studio issues a Privacy Notice to all learners and or parents, this summarises the information held of learners, why it is held and the other organisations to who it may be passed on to.

Purpose

This policy sets out how Playback Studio deals with personal information correctly and securely and in accordance with the Data Protection Act 1998, and other related legislation.

This policy applies to all personal information however it is collected, used, recorded and stored and whether it is held on paper or electronically.

All staff involved with the collection, use, processing or disclosure of personal data will be aware of their duties and responsibility and will adhere to this policy.

What personal information / data

Personal information or data is information which relates to a living individual who can be identified from that data, or from that data in addition to other information available to them. Personal data included (but is not limited to) an individual's name, address, date of birth, photograph, bank details and other information that identifies them.

Data Protect Principles

The Data Protection Act 1998 establishes eight principles that must always be adhered to:

1. Personal data shall be processed fairly and lawfully.
2. Personal data shall be obtained only for one or more specified and lawful purposes.
3. Personal data shall be adequate, relevant and not excessive.
4. Personal data shall be accurate and where necessary, kept up to date.
5. Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose or purposes.

6. Personal data shall be kept secure i.e. protected by an appropriate degree of security.

7. Personal data shall not be transferred to a country or territory outside the European Economic area unless that country or territory ensures an adequate level of protection.

Commitment

Playback Studio is committed to always maintaining the above principles. Therefore, we will;

- Inform individuals why personal information is being collected

- Inform individuals when their information is shared and why, and with whom, unless the Data Protection Act provides a reason not to do this.

- Check the accuracy of the information it holds and review it at regular intervals.

- Ensure that clear and robust safeguards are in place to ensure personal information is kept securely and to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded.

- Ensure that personal information is not retained longer than it is needed - Ensure that when information is destroyed that it is done so appropriately and securely.

- Share personal information with others only when it is legally appropriate to do so.

- Comply with the duty to respond to requests for access to personal information, known as Subject Access Requests.

- Ensure that personal information is not transferred outside the EEA without the appropriate safeguards.

- Ensure all staff and governors are aware of and understand these policies and procedures.

Learner Obligations

Learners must ensure that all personal data provided to Playback Studio is accurate and up to date. They must ensure that changes of address etc are updated on the learner registration system.

Learners may, as part of a project, process personal data. If they do so they must comply with the Playback Studio's Data Protection Policy.

The Data Controller and the Data Protection Officer

Playback Study as a body corporate is the data controller under the Act, and the Directors are therefore ultimately responsible for implementation. However, the Data Protection Officer will deal with day-to-day matters.

Playback Studio has designated Kes Charles (Director) to act as Data Protection Officer. Any query relating to the implementation within Playback Studio of the Act and Subject Access Requests under section 7 of the Act should be referred to Legal Services.

Privacy Notice – Your Personal Learner Record (PLR)

A personal learning record (PLR) is an online compilation of a person's learning and achievement records collected by UK education bodies, held by the Learning Records Service (LRS). The information stored in your PLR is provided by the Skills Funding Agency in partnership with other educational organisations that you have agreed can collect and share information on your behalf.

The PLR allows you to access a government-backed record of what you have learned and achieved through education and employment. The PLR will be a lifelong record of your learning and qualifications, which will be accessible to you and to organisations where you have permitted viewing.

The PLR service supports Playback Studio and other awarding organisations in their ability to make awards of qualifications based on units awarded by other awarding organisations. The PLR service may obtain personal information that has been obtained by third parties to supplement your PLR.

All organisations that will have access to the information you provide are registered under the Data Protection Act 1998 and will use your personal information in accordance with requirements of the Act. At no time will your personal information be passed to organisations for marketing or sales purposes.

For further details of how your data is shared and used by the Learner Registration Service and how to change who has access to your record, please go to https://www.gov.uk/government/publications/learning-records-service-the-plr-forlearners-and-parents

The National Careers Service also provides access to your PLR, information, advice and guidance tools to help you make decisions on learning, training and work opportunities.

LRS: https://www.gov.uk/government/publications/learning-records-service-the-plr-forlearners-and-parents

NCS: https://nationalcareersservice.direct.gov.uk/about-us/home

Examination Marks

Learners will be entitled to information about their marks for both coursework and examinations as part of their tutorial support. This is within the provisions of the Act relating to the release of data. However, this may take longer than other information to provide.

Security

All staff are made aware of the security procedures they must follow when handling personal information. Information is protected from unauthorised access, and we are confident no one will be able to access your personal information unlawfully. We also protect information which is being transferred. Please note that an email is never a 100% secure way of communicating. By using it, you agree that you will send any information by email at your own risk.

While we will take all reasonable precautions to make sure that other organisations who we deal with have good security practices, we are not responsible for the privacy practices of those organisations whose may be linked to our service.

Playback Studio Learner Collection Notice

We are obliged to make this notice available to you as part of our own Data Protection Policy

Induction and end of programme learner surveys

Your details may be requested when completing a Playback induction or end of programme survey.

About six months after you complete the programme, we may contact you to ask you to complete a 'Destinations of Learners' questionnaire. You may also be contacted as part of an audit to check that we have undertaken our programme within the quality of our organisation and funders.

If you do not want to take part in any of these surveys, please let us know.

Submission of your information to Playback Studio

Each year we will send some of the information we hold about you to our funders. Our funders collect, and is responsible for, the database in which your Playback Studio information is stored. Our funders include European Social Fund, Prevista, Ground works and prospects. Playback Studio may use your information to evaluate the quality of the programmes delivered or to produce statistics for publication. Out funders may use your details for its own purposes or share your information with third parties. Our funders may charge other organisations to whom it provides services and data. All uses of your information must comply with the Data Protection Act 1998. www.legislation.gov.uk/ukpga/1998/29/contents.

Sensitive information

If you give us information about your disability status, ethnicity, sexual orientation, gender reassignment or religion, this may be included in the information we have about you. It may be used to assist with monitoring equality of opportunity and eliminating unlawful discrimination in accordance with the Equality Act. Some other sensitive information is used to enable research into the provision of fair access to learning, for example information as to whether you are a care leaver.

Your sensitive information will not be used to make decisions about you or used for the purposes below:

Purpose 1 - Education statistics and data

Your information may be used by some organisations to help carry out public functions connected with education and learning in the UK. These organisations are data controllers in common of your information under the terms of the Data Protection Act (this link explains what this means ico.org.uk/for-organisations/guide-to-data-protection/key definitions/). Such organisations may include:

Department for Business, Innovation and Skills

Department for Employment and Learning

Department for work and Pensions

Department for Skills and Education

Department for of Social Security

Local Authority Social Service departments

Research Councils

Education Funding Agency

European Social Fund

National Health Service

Other uses

Your information may also be used by some organisations who are also data controllers in common to help carry out public functions that are not connected with education and learning. Such uses may include the following:

- Measurement of population levels and migration by the Office for National Statistics
- National Records of England
- Office for National Statistics
- Monitoring of public expenditure by the National Audit Office
- Monitoring of the accuracy of electoral registers by Electoral Registration Officials.

Purpose 2 - Administrative uses

Fraud detection and prevention

Your information may be used to audit claims to public funding and student finance, and to detect and prevent fraud.

Previous study

If you have ever enrolled on a further education or higher education course. The Higher Education Funding Council for England (HEFCE) may share your previous education records with us, including, information submitted by other institutions, to determine the nature of any prior education study, including your possible current qualifications. This may be used to make decisions learning you may or may not have to do, the support available to you or the availability of a place for you to study with us.

Your information will not be used to make decisions about you other than for those uses outlined under Purpose 2.

Purpose 3 – Playback Studio publications

Playback Studio may use your information to produce and publish information and statistics. This includes some National Statistics publications (www.statisticsauthority.gov.uk/nationalstatistician/types-of-official-statistics) and online business intelligence and research services. Playback Studio will take precautions to ensure that individuals are not identified from any information which is processed for such publications.

Purpose 4 - Equal opportunity, research, journalism, and other processing in which there is a legitimate interest

Playback Studio and the other data controllers in common (see Purpose 1) may also supply information to third parties where there is a legitimate interest in doing so. Examples of use for this purpose include:

• Equal opportunities monitoring

• Research - This may be academic research, commercial research or other statistical research where this is in the public interest

• Journalism - Where the relevant publication would be in the public interest e.g. league tables

• Provision of information to learners and prospective learners.

Users to whom information may be supplied for Purpose 4 include:

• Higher education sector bodies

• Higher education providers

• Academic researchers and students

• Commercial organisations (e.g. recruitment firms, housing providers, graduate employers)

• Unions • Non-governmental organisations and charities

• Local, regional and national government bodies

• Journalists

Information supplied by Playback Studio to third parties within Purpose 4 is supplied under contracts which require that individuals shall not be identified from the supplied information. If you would like information on current agreements Playback Studio has to supply of information to external agencies, please contact a director at info@playbackstudio.co.uk.

Access to your data

Under the Data Protection Act, you have the right to receive a copy of the personal data we have about you. If you want a copy, please write to:

Playback Studio, The Stephan Lawrence Centre, 39 Brookmill Road, London, SE8 4HU

You may have to pay a fee for this.

Retention of Data

Playback Studio will keep some forms of information for longer than others.

Data on learners, including any information on health, race or disciplinary matters, will be destroyed after 10 years but a skeletal record will be retained to include a full transcript of academic achievements.

Playback Studio will need to keep central personnel records indefinitely. This will include information necessary in respect of pensions, taxation, potential or current disputes or litigation regarding the employment, and information required for job references.

Research data must be retained in accordance with the Code of Practice for Research.

Compliance

Compliance with the Act is the responsibility of all members of Playback Studio. Any deliberate breach of the data protection policy may lead to disciplinary action being taken, or access to Playback Studios facilities being withdrawn, or even a criminal prosecution. It may also result in personal liability for the individual. Any questions or concerns about the interpretation or operation of this policy should be taken up with the Data Protection Officer.

This policy was approved by Playback Studio on 12th December 2017 and takes immediate effect.

Complaints

Complaints will be dealt with in accordance with Playback's appeal policy.

Complaints relating to the handling of personal information may be referred to the Information Commissioner who can be contacted at Wycliffe House, Water Lane Wilmslow Cheshire SK9 5AF or at www.ico.gov.uk

Appendix

Data Protection Act 1998

Guidelines for Staff – Appendix 1

1. Members of staff will process personal data on a regular basis. Playback Studio will ensure that staff and learners give their consent to processing, or that another condition for processing applies, and are notified of the categories of processing, as required by the Act.

2. Information about an individual's physical or mental health; sexual life; political or religious views; trade union membership; ethnicity or race; the commission of criminal offences and court proceedings dealing with criminal offences is sensitive and can normally only be collected and processed with their express consent.

3. Members of staff have a duty to make sure that they comply with the data protection principles, which are set out in Playback Studio Data Protection Policy. In particular, staff must ensure that records are;

- Accurate
- up-to-date
- fair
- kept and disposed of safely
- and in accordance with Playback Studio policy

4. Individual members of staff are responsible for ensuring that all data they are holding is kept securely.

5. Members of staff must not disclose personal data, unless for normal academic, administrative or pastoral purposes, without authorisation or agreement from the Data Protection Officer, or in line with Playback Studio policy.

6. Members of staff must complete Playback Studio registrations forms in respect of all databases holding personal data before commencing processing of the data.

7. Before processing any personal data, all staff should consider the checklist.

8. All staff should make themselves aware of the Data Protection Toolkit and other resources.

PLAYBACK

Staff Checklist for Recording Data

- Do you really need to record the information?
- Is the information 'standard' or is it 'sensitive'?
- If it is sensitive, do you have the data subject's express consent?
- Has the individual or data subject been told that this type of data will be processed?
- Are you authorised to collect/store/process the data?
- If yes, have you checked with the data subject that the data is accurate?
- Are you sure that the data is secure?
- If you do not have the data subject's consent to process, are you satisfied that one of the other conditions for processing data applies?
- In respect of databases containing personal data, have you notified Playback Directors that you intend to hold the data and registered the database?
- How long do you need to keep the data for, and what is the mechanism for review/destruction?

Glossary of Terms

Data

Any information held by Playback Studio for the purposes of Playback Studio business.

Personal Data

Information about a living person. This information is protected by the Act.

Data Subject

The person about whom the data are held.

Sensitive Data

The Act introduces categories of sensitive personal data, namely, personal data consisting of information as to:

1. the racial or ethnic origin of the data subject,
2. their political opinions,
3. their religious beliefs or other beliefs of a similar nature,
4. whether they are a member of a trade union,
5. their physical or mental health or condition,
6. their sexual life,
7. the commission or alleged commission by them of any offence, or
8. any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings.

Data Controller

A person (or organisation) who determines the purposes for which, and the manner in which, any personal data are, or are to be, processed.

Processing

Covers almost anything which is done with or to the data, including:

- obtaining data
- recording or entering data onto the files
- holding data, or keeping it on file without doing anything to it or with it
- organising, altering or adapting data in any way
- retrieving, consulting or otherwise using the data
- disclosing data either by giving it out, by sending it on email, or simply by making it available
- combining data with other information
- erasing or destroying data

Useful resources

- The Information Commissioner's Officer's website contains guidance on data protectionhttps://ico.org.uk/for-organisations/guide-to-data-protection/
- https://ico.org.uk/for-organisations/resources-and-support/data-protection-selfassessment/

General data protection regulation (GDPR) policy

This policy links to and should be read in conjunction with the following policies:

- IT Security Policy
- CCTV Policy and Procedure
- ICT usage policy
- Learner, staff and employer privacy notices

1. Introduction

1.1 Playback Studio is required to keep and process certain information about its staff members, pupils and others in accordance with its legal obligations under the General Data Protection Regulation (GDPR).

1.2 Playback Studio may, from time to time, be required to share personal information about its staff or

pupils with other organisations, mainly the local authority, other educational bodies and services.

1.3 This policy is in place to ensure all staff, contractors and sub-contractors are aware of their responsibilities and outlines how Play back Studio complies with the following core principles of the GDPR.

1.4 Organisational methods for keeping data secure are imperative, and Playback Studio believes that it is good practice to keep clear practical policies, backed up by written procedures.

1.5 This policy complies with the requirements set out in the GDPR, which came into effect on 25 May 2018.

2. Legal framework

2.1 This policy has due regard to legislation, including, but not limited to the following:

• General Data Protection Regulation (GDPR)

• Freedom of Information Act 2000

• Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)

• Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004

• Training Standards and Framework Act 1998

2.2 This policy will also have regard to the following guidance:

• Information Commissioner's Office (2017) 'Overview of the General Data Protection Regulation (GDPR)' • Information Commissioner's Office (2017) 'Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now'

3. Applicable data

3.1 For the purpose of this policy, personal data refers to information that relates to an identifiable, living individual, including information such as an online identifier, e.g. an IP address. The GDPR applies to both automated personal data and to manual filing systems, where personal data is accessible according to specific criteria, as well as to chronologically ordered data and pseudonymised data, e.g. key-coded.

3.2 Sensitive personal data is referred to in the GDPR as 'special categories of personal data', which are broadly the same as those in the Data Protection Act (DPA) 1998. These specifically include the processing of genetic data, biometric data and data concerning health matters.

4. Principles

4.1 In accordance with the requirements outlined in the GDPR, personal data will be:

a) Processed lawfully, fairly and in a transparent manner in relation to individuals.

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.

c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

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.

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 GDPR in order to safeguard the rights and freedoms of individuals.

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.

g) The GDPR also requires that “the controller shall be responsible for, and able to demonstrate, compliance with the principles”.

5. Accountability

5.1 Playback Studio will implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the GDPR. We will provide comprehensive, clear and transparent privacy policies.

5.2 Records will be kept in line with funding body contractual requirements including retention periods specified by them.

5.3 Playback Studio will implement measures that meet the principles of data protection by design and data protection by default, such as:

a) Data minimisation.

b) Pseudonymisation.

c) Transparency.

d) Allowing individuals to monitor processing.

e) Continuously creating and improving security features.

6.3 Data protection impact assessments will be used, where appropriate.

6. Data protection officer (DPO)

6.1 A DPO will be appointed in order to:

• Inform and advise Playback Studio and its employees and sub-contractors about their obligations to comply with the GDPR and other data protection laws.

• Monitor Playback Studio's compliance with the GDPR and other laws, including managing internal data protection activities, advising on data protection impact assessments, conducting internal audits, and providing the required training to staff members.

6.2 An existing employee will be appointed to the role of DPO provided that their duties are compatible with the duties of the DPO and do not lead to a conflict of interests.

6.3 The individual appointed as DPO will have professional experience and knowledge of data protection law, particularly that in relation to education.

6.4 The DPO will be a member of the SMT

6.5 The DPO will operate independently and will not be dismissed or penalised for performing their task.

6.6 Sufficient resources will be provided to the DPO to enable them to meet their GDPR obligations.

7. Lawful processing

7.1 The legal basis for processing data will be identified and documented prior to data being processed and in most cases will be legitimate interest or explicit consent

7.2 Under the GDPR, data will be lawfully processed under the following conditions:

• The consent of the data subject has been obtained.

• Or, processing is necessary for: ¾ Compliance with a legal obligation. ¾ The performance of a task carried out in the public interest or in the exercise of official authority vested in the controller e.g. education

- For the performance of a contract with the data subject or to take steps to enter into a contract.
- Protecting the vital interests of a data subject or another person.
- For the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject.

7.3 Sensitive data will only be processed under the following conditions:

• Legitimate interest or explicit consent of the data subject, unless reliance on consent is prohibited by EU or Member State law.

• Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent.

• Processing relates to personal data manifestly made public by the data subject.

• Processing is necessary for:

- Carrying out obligations under employment, social security or social protection law, or a collective agreement.
- Protecting the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent.
- The establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity.
- Reasons of substantial public interest on the basis of Union or Member State law which is proportionate to the aim pursued and which contains appropriate safeguards.
- The purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional.
- 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 healthcare and of medicinal products or medical devices. ¾ Archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1).

8. Consent

8.1 Consent must be a positive indication. It cannot be inferred from silence, inactivity or preticked boxes.

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

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

8.4 Playback ensures that consent mechanisms meet the standards of the 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.

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

8.6 Consent can be withdrawn by the individual at any time.

8.7 Where a child is under the age of 13, the consent of parents will be sought prior to the processing of their data, except where the processing is related to preventative or counselling services offered directly to a child.

9. The right to be informed

9.1 The privacy notice supplied to individuals in regards to the processing of their personal data will be

written in clear, plain language which is concise, transparent, easily accessible and free of charge.

9.2 In relation to data obtained both directly from the data subject and not obtained directly from the data subject, the following information will be supplied within the privacy notice:

• The identity and contact details of the controller (and where applicable, the controller's representative) and the DPO.

• The purpose of, and the legal basis for, processing the data.

• The legitimate interests of the controller or third party.

• Any recipient or categories of recipients of the personal data.

• Details of transfers to third countries and the safeguards in place.

• The retention period of criteria used to determine the retention period.

• The existence of the data subject's rights, including the right to:

• Withdraw consent at any time.

• Lodge a complaint with a supervisory authority.

• The existence of automated decision making, including profiling, how decisions are made, the significance of the process and the consequences.

9.3 Where data is obtained directly from the data subject, information regarding whether the provision of personal data is part of a statutory or contractual requirement, as well as any possible consequences of failing to provide the personal data, will be provided.

9.4 Where data is not obtained directly from the data subject, information regarding the categories of personal data that Playback Studio holds, the source that the personal data originates from and whether it came from publicly accessible sources, will be provided.

9.5 For data obtained directly from the data subject, this information will be supplied at the time the data is obtained.

9.6 In relation to data that is not obtained directly from the data subject, this information will be supplied:

• Within one month of having obtained the data.

• If disclosure to another recipient is envisaged, at the latest, before the data are disclosed.

• If the data are used to communicate with the individual, at the latest, when the first communication takes place.

10. The right of access

10.1 Individuals have the right to obtain confirmation that their data is being processed.

10.2 Individuals have the right to submit a subject access request (SAR) to gain access to their personal data in order to verify the lawfulness of the processing.

10.3 Playback will verify the identity of the person making the request before any information is supplied.

10.4 A copy of the information will be supplied to the individual free of charge; however, Playback Studio may impose a 'reasonable fee' to comply with requests for further copies of the same information.

10.5 Where a SAR has been made electronically, the information will be provided in a commonly used electronic format.

10.6 Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged.

10.7 All fees will be based on the administrative cost of providing the information.

10.8 All requests will be responded to without delay and at the latest, within one month of receipt.

10.9 In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension, and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.

10.10 Where a request is manifestly unfounded or excessive, Playback Studio holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal.

10.11 In the event that a large quantity of information is being processed about an individual, Playback Studio will ask the individual to specify the information the request is in relation to.

11. The right to rectification

11.1 Individuals are entitled to have any inaccurate or incomplete personal data rectified.

11.2 Where the personal data in question has been disclosed to third parties, Playback Studio will inform them of the rectification where possible.

11.3 Where appropriate, Playback Studio will inform the individual about the third parties that the data has been disclosed to.

11.4 Requests for rectification will be responded to within one month; this will be extended by two months where the request for rectification is complex.

11.5 Where no action is being taken in response to a request for rectification, Playback Studio will explain the reason for this to the individual, and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

12. The right to erasure

12.1 Individuals hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

12.2 Individuals have the right to erasure in the following circumstances:

a) Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed

b) When the individual withdraws their consent

c) When the individual objects to the processing and there is no overriding legitimate interest for

continuing the processing

d) The personal data was unlawfully processed

e) The personal data is required to be erased in order to comply with a legal obligation

f) The personal data is processed in relation to the offer of information society services to a child

12.3 Playback Studio has the right to refuse a request for erasure where the personal data is being processed for the following reasons:

a) To exercise the right of freedom of expression and information

b) To comply with a legal obligation for the performance of a public interest task or exercise of official authority

c) For public health purposes in the public interest

d) For archiving purposes in the public interest, scientific research, historical research or statistical purposes

e) The exercise or defence of legal claims

12.4 As a child may not fully understand the risks involved in the processing of data when consent is obtained, special attention will be given to existing situations where a child has given consent to processing and they later request erasure of the data, regardless of age at the time of the request.

12.5 Where personal data has been disclosed to third parties, they will be informed about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.

12.6 Where personal data has been made public within an online environment, the Training will inform other organisations who process the personal data to erase links to and copies of the personal data in question.

13. The right to restrict processing

13.1 Individuals have the right to block or suppress Playback Studio's processing of personal data.

13.2 In the event that processing is restricted, Play Back Studio will store the personal data, but not further process it, guaranteeing that just enough information about the individual has been retained to ensure that the restriction is respected in future.

13.3 Playback Studio will restrict the processing of personal data in the following circumstances:

• Where an individual contests the accuracy of the personal data, processing will be restricted until Playback Studio has verified the accuracy of the data

• Where an individual has objected to the processing and Playback Studio is considering whether their legitimate grounds override those of the individual

• Where processing is unlawful and the individual opposes erasure and requests restriction instead

• Where Playback Studio no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim

13.4 If the personal data in question has been disclosed to third parties, Playback Studio will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.

13.5 Playback Studio will inform individuals when a restriction on processing has been lifted.

14. The right to data portability

14.1 Individuals have the right to obtain and reuse their personal data for their own purposes across different services.

14.2 Personal data can be easily moved, copied or transferred from one IT environment to another in a safe and secure manner, without hindrance to usability.

14.3 The right to data portability only applies in the following cases:

• To personal data that an individual has provided to a controller

• Where the processing is based on the individual's consent or for the performance of a contract

• When processing is carried out by automated means

14.4 Personal data will be provided in a structured, commonly used and machine-readable form.

14.5 Playback Studio will provide the information free of charge.

14.6 Where feasible, data will be transmitted directly to another organisation at the request of the individual.

14.7 Playback Studio is not required to adopt or maintain processing systems which are technically compatible with other organisations.

14.8 In the event that the personal data concerns more than one individual, Playback Studio will consider whether providing the information would prejudice the rights of any other individual.

14.9 Playback Studio will respond to any requests for portability within one month.

14.10 Where the request is complex, or several requests have been received, the timeframe can be extended by two months, ensuring that the individual is informed of the extension and the reasoning behind it within one month of the receipt of the request.

14.11 Where no action is being taken in response to a request, Playback Studio will, without delay and at the latest within one month, explain to the individual the reason for this and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

15. The right to object

15.1 Playback Studio will inform individuals of their right to object at the first point of communication, and this information will be outlined in the privacy notice and explicitly brought to the attention of the data subject, ensuring that it is presented clearly and separately from any other information.

15.2 Individuals have the right to object to the following:

• Processing based on legitimate interests or the performance of a task in the public interest

• Direct marketing

• Processing for purposes of scientific or historical research and statistics.

15.3 Where personal data is processed for the performance of a legal task or legitimate interests:

• An individual's grounds for objecting must relate to his or her particular situation.

• Playback Studio will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where Playback Studio can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.

15.4 Where personal data is processed for direct marketing purposes:

• Playback Studio will stop processing personal data for direct marketing purposes as soon as an objection is received.

• Playback Studio cannot refuse an individual's objection regarding data that is being processed for direct marketing purposes.

15.5 Where personal data is processed for research purposes:

• The individual must have grounds relating to their particular situation in order to exercise their right to object.

• Where the processing of personal data is necessary for the performance of a public interest task, Playback Studio is not required to comply with an objection to the processing of the data.

• Where the processing activity is outlined above, but is carried out online, Playback Studio will offer a method for individuals to object online.

16. Automated decision making and profiling

16.1 Individuals have the right not to be subject to a decision when:

• It is based on automated processing, e.g. profiling.

• It produces a legal effect or a similarly significant effect on the individual.

16.2 Playback Studio will take steps to ensure that individuals are able to obtain human intervention, express their point of view, and obtain an explanation of the decision and challenge it.

16.3 When automatically processing personal data for profiling purposes, Playback Studio will ensure that the appropriate safeguards are in place, including:

• Ensuring processing is fair and transparent by providing meaningful information about the logic involved, as well as the significance and the predicted impact.

• Using appropriate mathematical or statistical procedures.

• Implementing appropriate technical and organisational measures to enable inaccuracies to be corrected and minimise the risk of errors.

• Securing personal data in a way that is proportionate to the risk to the interests and rights of the individual and prevents discriminatory effects.

16.4 Automated decisions must not concern a child or be based on the processing of sensitive data, unless:

• Playback Studio has the explicit consent of the individual.

• The processing is necessary for reasons of substantial public interest on the basis of Union/Member State law.

17. Privacy by design and privacy impact assessments

17.1 Playback Studio will act in accordance with the GDPR by adopting a privacy by design approach and implementing technical and organisational measures which demonstrate how Playback Studio has considered and integrated data protection into processing activities.

17.2 Data protection impact assessments (DPIAs) will be used to identify the most effective method of complying with Playback Studio's data protection obligations and meeting individuals' expectations of privacy.

17.3 DPIAs will allow Playback Studio to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to Playback Studio's reputation which might otherwise occur.

17.4 A DPIA will be carried out when using new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals.

17.5 A DPIA will be used for more than one project, where necessary.

17.6 High risk processing includes, but is not limited to, the following:

a) Systematic and extensive processing activities, such as profiling

b) Large scale processing of special categories of data or personal data which is in relation to criminal convictions or offences

c) The use of CCTV.

17.7 Playback Studio will ensure that all DPIAs include the following information:

a) A description of the processing operations and the purposes

b) An assessment of the necessity and proportionality of the processing in relation to the purpose

c) An outline of the risks to individuals

d) The measures implemented in order to address risk

17.8 Where a DPIA indicates high risk data processing, Playback Studio will consult the ICO to seek its opinion as to whether the processing operation complies with the GDPR.

18. Data breaches

18.1 The term 'personal data breach' refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

18.2 The SMT will ensure that all staff members are made aware of, and understand, what constitutes a data breach as part of their CPD training.

18.3 Where a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed.

18.4 All notifiable breaches will be reported to the relevant supervisory authority within 72 hours of Playback Studio becoming aware of it.

18.5 The risk of the breach having a detrimental effect on the individual, and the need to notify the relevant supervisory authority, will be assessed on a case-by-case basis.

18.6 In the event that a breach is likely to result in a high risk to the rights and freedoms of an individual, Playback Studio will notify those concerned directly.

18.7 A 'high risk' breach means that the threshold for notifying the individual is higher than that for notifying the relevant supervisory authority.

18.8 In the event that a breach is sufficiently serious, the public will be notified without undue delay.

18.9 Effective and robust breach detection, investigation and internal reporting procedures are in place at Playback Studio, which facilitate decision-making in relation to whether the relevant supervisory authority or the public need to be notified.

18.10 Within a breach notification, the following information will be outlined:

a) The nature of the personal data breach, including the categories and approximate number of individuals and records concerned

b) The name and contact details of the DPO

c) An explanation of the likely consequences of the personal data breach

d) A description of the proposed measures to be taken to deal with the personal data breach

e) Where appropriate, a description of the measures taken to mitigate any possible adverse effects

18.11 Failure to report a breach when required to do so may result in a fine, as well as a fine for the breach itself.

19. Data security

19.1 Confidential paper records will be kept in a locked filing cabinet, drawer or safe, with restricted access.

19.2 Confidential paper records will not be left unattended or in clear view anywhere with general access.

19.3 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.

19.4 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.

19.5 Memory sticks will not be used to hold personal information unless they are password protected and fully encrypted.

19.6 All electronic devices are password-protected to protect the information on the device in case of theft.

19.7 Where possible, Playback Studio enables electronic devices to allow the remote blocking or deletion of data in case of theft.

19.8 Where staff use their personal laptops or computers Playback Studio purposes this must be in accordance with the ICT usage policy

19.9 All necessary members of staff are provided with their own secure login and password, and every computer regularly prompts users to change their password.

19.10 Emails containing sensitive or confidential information are password-protected if there are unsecure servers between the sender and the recipient.

19.11 Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.

19.12 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 from Playback Studio premises accepts full responsibility for the security of the data.

19.13 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 has been outlined in a privacy notice.

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

19.15 The physical security of Playback Studio ’s buildings and storage systems, and access to them, is reviewed on a termly basis as per Playback Studio’s IT Security Policy. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place.

19.16 Playback Studio takes its duties under the GDPR seriously and any unauthorised disclosure may result in disciplinary action.

19.17 The IT Manager is responsible for having continuity and recovery measures in place to ensure the security of protected data.

19.18 Where staff are taking data out of company premises in any form including devices such as laptops, mobiles, storage devices etc. as well as records in other formats such as paper enrolment forms etc., they are responsible for ensuring the security of that data. All data or devices which contain data must be kept on their person or in locked storage the whole time they are offsite. No data or devices may be left in an unoccupied car at any time and all data or devices must be taken into a building or kept about their person when the car is left unattended.

20. Publication of information

20.1 Playback Studio will not publish any personal information, including photos, on its website without the permission of the affected individual.

20.2 When uploading information to the Playback Studio website, staff are considerate of any metadata or deletions which could be accessed in documents and images on the site.

21. CCTV and photography

21.1 Playback Studio understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles.

21.2 Playback Studio notifies all pupils, staff and visitors of the purpose for collecting CCTV images via notice boards, letters and email.

21.3 Cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose.

21.4 All CCTV footage will be kept for three months for security purposes; the IT Manager is responsible for keeping records and the Data Protection Officer is responsible for allowing access. Details are set out in Playback Studio's CCTV Policy.

21.5 Playback Studio will always indicate its intentions for taking photographs or video of learners and will request consent before publishing them.

21.6 Images captured by individuals for recreational/personal purposes, and videos made by parents for family use, are exempt from the GDPR.

22. Data retention

22.1 Data will not be kept for longer than is necessary.

22.2 Unrequired data will be deleted as soon as practicable.

22.3 Some educational records relating to former pupils or employees of Playback Studio may be kept for an extended period for legal reasons, but also to enable the provision of references or academic transcripts.

22.4 Paper documents will be shredded or pulped, and electronic memories scrubbed clean or destroyed, once the data should no longer be retained.

23. DBS data

23.1 All data provided by the DBS will be handled in line with data protection legislation; this includes electronic communication.

23.2 Data provided by the DBS will never be duplicated.

23.3 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.

REVIEW DATES AND APPROVAL

Date of last review: January 2024	Date of next review: January 2025