The GALLERY TRUST

A community of special schools

Data Protection Policy

Policy Owner	CFOO
Approved by	Financial and Personnel Committee
Date approved	May 2026
Date of next review	May 2028
Signed:	Chief Executive Officer:  Chair of Trustees: 

Contents

1. Aims

The Gallery Trust aims to ensure that all personal data collected about staff, pupils, parents, trustees, members, Local Academy Board members, visitors and other individuals is collected, stored and processed in accordance with both the Data Protection Act 2018 (DPA) and the General Data Protection Regulation (GDPR) and statutory guidance by all establishments in the organisation. All establishments in the organisation are referred to as the 'Trust' in this policy.

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

2. Legislation and guidance

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

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

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

3. Definitions

Term	Definition
Personal Data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special Categories of Personal Data	Personal data, which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sexual orientation • Gender

Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or
Data Subject	The identified or identifiable individual whose personal data is held or processed.
Data Controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data Processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.
DPIA	It is a structured risk assessment for how your use of data could harm individuals, and how you will prevent that harm
Giving Consent	freely, clearly, and knowingly agreeing to the processing of your personal data for a specific purpose
Opt Out	formally withdrawing or refusing permission for your personal data to be used, stopping that processing where the law allows

4. Legislative Framework

UK General Data Protection Regulation (UK GDPR)
is the UK's version of the GDPR, retained in domestic law. It sets out core data protection principles, rights and obligations, and is supplemented by the DPA 2018. The

EU General Data Protection Regulation (EU GDPR)
applies within the European Union.

Data Protection Act 2018 (DPA 2018)
is the UK's primary data protection legislation. It sits alongside and supplements the UK GDPR, including UK- specific provisions, exemptions and enforcement arrangements.

Data (Use and Access) Act 2025 (DUAA)
amends data protection, digital verification and smart data frameworks. Key education-sector changes include the ability to pause subject access request timescales during school holidays ('stop the clock'), a statutory reasonable and proportionate test for compliance with information rights.

Freedom of Information Act 2000 (FOIA)
provides a general right of access to recorded information held by public authorities, subject to statutory exemptions.

Protection of Freedoms Act 2012 (PoFA 2012)
regulates, among other things, the use of biometric data and surveillance, including requirements for consent and governance.

Education (Pupil Information) (England) Regulations 2005
set out parents' rights to access their child's educational records and schools' duties to disclose them.

Education Act (EA)
sets the legal framework for the organisation, administration and provision of education in England, including school governance, curriculum, attendance and funding.

Information Commission (IC)
is the UK's independent regulator for data protection, freedom of information and related rights. It ensures compliance with the Data Protection Act, the Freedom of Information Act, and the UK GDPR, and handles formal complaints. (Formerly known as the Information Commissioner's Office (ICO); renamed under the Data (Use and Access) Act 2025.)

Keeping Children Safe in Education (KCSIE)
is statutory guidance for schools and colleges in England on safeguarding and safer recruitment, issued by the Department for Education (DFE).

5. The Data Controller

The Trust determines the purposes and means of processing personal data, and therefore is a data controller.

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

6. Roles and responsibilities

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

6.1 Board of Trustees

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

6.2 Data Protection Officer

The Data Protection Officer (DPO) is responsible for overseeing the implementation of this policy, monitoring compliance with data protection law, and developing related policies and guidelines where applicable. All queries regarding data protection issues should be referred to the DPO.

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

The Gallery Trust's DPO is Satswana Ltd, info@satswana.com; telephone number 01252 759177.

6.3 Head Teacher / Head of Establishment

The Head of Establishment acts as the representative of the data controller on a day-to-day basis for the establishment.

6.4 All Staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the Trust of any changes to their personal data, such as a change of address
- Contacting the Head of Establishment regarding data protection requests and concerns
- Contacting the DPO in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - To seek guidance regarding processing data protection requests, e.g. SAR
    - If they have any concerns that this policy is not being followed
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
    - If there has been a data breach
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
    - If they need help with any contracts or sharing personal data with third parties

7. Data Protection Principles

The GDPR is based on data protection principles that the Trust must comply with.

The principles say that personal data must be:

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

8. Collecting Personal Data

8.1 Lawfulness, Fairness and transparency

The Trust will only process personal data where there is one of 6 ‘lawful bases’ (legal reasons)

to do so under data protection law:

- The data needs to be processed so that the Trust can **fulfil a contract** with the individual, or the individual has asked the Trust to take specific steps before entering into a contract

- The data needs to be processed so that the Trust can **comply with a legal obligation**

- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life

- The data needs to be processed so that the Trust, as a public authority, can perform a task **in the public interest,** and carry out its official functions

- The data needs to be processed for the **legitimate interests** of the Trust or a third party (provided the individual's rights and freedoms are not overridden)

- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**

For special categories of personal data, the Trust will also meet one of the special category conditions for processing which are set out in the GDPR.

If the Trust offer online services to pupils, such as classroom apps, and the Trust intend to rely on consent as a basis for processing, parental consent will be obtained where the pupil is under 13 (except for online counselling and preventive services).

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

8.2 Limitation, Minimisation and Accuracy

The Trust will only collect personal data for specified, explicit and legitimate reasons. The Trust will explain these reasons to the individuals when data is collected.

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

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

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised.

9. Sharing Personal Data

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

- There is an issue with a pupil or parent/carer that puts the safety of staff or pupils at risk

- The need to liaise with other agencies

- The Trust's suppliers or contractors need data to enable the Trust to provide services to staff and pupils – for example, IT companies. When doing this, the Trust will:

- Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law

- Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe

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

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

The Trust may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects pupils or staff.

10. Subject access requests and other rights of individuals

10.1 Subject access requests

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

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

How to make a request:
Subject access requests can be submitted in any form (writing, email, phone, or in person). We can respond more quickly if you provide:
Your name

- Your address

- Contact number and email address
- Details of the information you want

If staff receive a subject access request they must immediately forward it to the DPO (info@satswana.com) and inform the Head of Establishment and the Digital Strategy and Network Manager.

Staff need to be aware that a subject access request may arrive in different formats. This can include the following:

Written in any format (Email, Letter, Web form, Messaging system etc.)
Subject Access Request through a representative
Subject Access Request made during another process (A grievance, complaint, legal claim, employment dispute, tribunal process)
Subject Access Request without a Explanation
Informal Subject Access Requests

10.2 Children and subject access requests

Safeguarding comes first:
We may refuse or restrict parental access where disclosure is likely to place a child or another person at risk of harm. This includes risks from domestic abuse, stalking, harassment, or coercive control. We make decisions case-by-case, considering safeguarding guidance and the child's best interests. We may consult the DSL and safeguarding partners.

Children's data belongs to them:
Personal data about a child belongs to that child, not their parents. For a parent to make a subject access request about their child, either:
The child must be unable to understand their rights and what a subject access request means, OR
The child must give explicit consent
For primary schools:
Children under 13 are generally not mature enough to understand their rights and subject access requests. We may usually grant requests from parents without the child's permission. However, we judge each child's ability to understand on a case-by-case basis.
For secondary schools:
Children aged 13 and above are generally mature enough to understand their rights and subject access requests. We will usually need the child's express permission before granting a parent's request. We judge each child's ability to understand on a case-by-case basis.

10.3 Responding to subject access requests

When responding to requests, the DPO:

- Will ask the individual to provide 2 forms of identification, including photo identification if it is necessary and proportionate
- May contact the individual via phone to confirm the request was made
- Will respond with the data without delay and within 1 month of receipt of the request
- Will provide the information free of charge
- May tell the individual the Trust will comply within 3 months of receipt of the request, where a request is complex or numerous.

The Trust will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

If the request is unfounded or excessive, the Trust may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.
A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information. Guidance must be taken from the DPO and Head of Establishment.

A subject access request belongs to the data subject. We will refuse a request if we believe it only benefits the person making the request and not the data subject.

In the event that the Trust refuses a request following consultation with the DPO and Head of Establishment, the Trust will tell the individual why, and tell them they have the right to complain to the ICO.

10.4 Other data protection rights of the individual

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

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

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

11. Parental requests to see the educational record

Those with parental responsibility may request access to a child's educational record under education regulations, but in England this statutory right applies only to local authority-maintained schools and all special schools, including those not maintained by a local authority. In academies, including free schools and independent schools, there is no automatic parental right of access unless the parent is lawfully entitled to act on the pupil's behalf under data protection law. All such requests must be treated as Subject Access Requests under UK GDPR and may be made in writing or verbally and will be considered on a case-by-case basis. Advice must be sought from the DPO and the Head of Establishment before any disclosure is made.

12. CCTV

The Trust uses CCTV in various locations around its sites to ensure it remains safe.

The Trust does not need to ask individuals' permission to use CCTV, but the Trust makes it clear where individuals are being recorded. Please refer to the Trust's CCTV policy.

Any enquiries about the CCTV system should be directed to the Head of Establishment in the first instance.

13. Photographs and videos

As part of school activities, photographs and record images of individuals within the establishments may be taken.

The Trust will obtain written consent from parents/carers, or pupils aged 13 and over, for photographs and videos to be taken of pupils for communication, marketing and promotional materials.

Where the Trust needs parental consent, it will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

Uses may include:

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

Consent can be refused or withdrawn at any time. If consent is withdrawn, the photograph or video will be deleted and not distributed further.

When using photographs and videos in this way no personal information about the child will be given, to ensure they cannot be identified.

14. Data protection by design and default

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

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing privacy impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Training members of staff on data protection law, this policy, any related policies and any other data protection matters; keeping a record of attendance
- Conducting reviews and audits to test privacy measures and make sure the Trust is compliant
- Maintaining records of processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our Trust and DPO and all information the Trust is required to share, about how personal data is processed (via privacy notices)
    - For all personal data held, maintaining an internal record of the type of data, data subject, how and why the data is used, any third-party recipients, how and why the data is stored, retention periods and how the data is kept safe

15. Data security and storage of records

The Trust will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage. Appropriate organisational and technical steps will be taken to secure data. In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals
- The Trust will aim to provide Encryption software to protect all portable devices as soon as possible
- Staff, pupils or governors who store personal information on their personal devices are

expected to follow the same security procedures as for school-owned equipment

- Where personal data is shared with a third party, the Trust will carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

16. Disposal of Records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely.

Paper-based records will be shredded, and electronic files will be deleted. The Trust may also use a third party to safely dispose of records on the school's behalf. The third party is required to provide sufficient guarantees that it complies with data protection law.

17. Personal Data Breaches

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

In the event of a suspected data breach, the procedure set out in appendix 1 will be followed.

When appropriate, the data breach will be reported to the ICO within 72 hours by the DPO.

Such breaches in a school context may include, but are not limited to:

- A non-anonymised dataset being published on the school website which shows the exam results of pupils eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about pupils

18. Training

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

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

Appendix 1: Personal Data Breach Procedure

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

On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO: Satswana Ltd, info@satswana.com; telephone number 01252 759177. The Head of Establishment and Digital Network and Strategy Manager must also be notified.

- The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people
- The DPO will advise on and make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
    - Loss of control over their data
    - Discrimination
    - Identify theft or fraud
    - Financial loss
    - Unauthorised reversal of pseudonymisation (for example, key-coding) to Damage to reputation
    - Loss of confidentiality
    - Any other significant economic or social disadvantage to the individual(s) concerned

If it is likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.

- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are provided to the Head of Establishment

- Where the ICO must be notified, the DPO will do this within 72 hours. As required, the DPO will set out:

    - A description of the nature of the personal data breach including, where possible:

        - The categories and approximate number of individuals concerned

        - The categories and approximate number of personal data records concerned

    - The name and contact details of the DPO

    - A description of the likely consequences of the personal data breach

    - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible

- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:

    - The name and contact details of the DPO

    - A description of the likely consequences of the personal data breach

    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s)concerned

- The DPO will notify any relevant third parties who can help mitigate the loss to individuals–for example, the police, insurers, banks or credit card companies

- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:

    - Facts and cause

    - Effects

    - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

Records of all breaches will be stored

- The DPO and Head of Establishment will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

Actions to minimise the impact of data breaches

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

Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error

- Members of staff who receive personal data sent in error must alert the sender, the DPO and Head of Establishment as soon as they become aware of the error

- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to recall it

- In any cases where the recall is unsuccessful, the Head of Establishment will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way

- The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request

- The DPO will carry out an internet search to check that the information has not been made public; if it has, the Trust will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted

Other types of breach could include:

- Details of pupil premium interventions for named children being published on the school website

- Non-anonymised pupil exam results or staff pay information being shared with governors

- A school laptop containing non-encrypted sensitive personal data being stolen or hacked

- The school's cashless payment provider being hacked and parents' financial details stolen

Appendix 2: Examinations Data Protection

This appendix details how The Gallery Trust, in relation to exams management and administration, ensures compliance with the regulations as set out by the Data Protection Act (DPA) and General Data Protection Regulation (GDPR).

Students are given the right to find out what information the Trust holds about them, how this is protected, how this can be accessed and how data breaches are dealt with.

All exams office staff responsible for collecting and sharing candidates' data are required to follow strict rules ensuring the information is:

- Used fairly and lawfully
- Used for limited, specifically stated purposes
- Used in a way that is adequate, relevant and not excessive
- Accurate and up to date
- Kept for no longer than is necessary
- Handled according to data subjects' data protection rights
- Kept safe and secure
- Not transferred outside the European Economic Area without adequate protection

Frameworks and References

This policy considers guidance and legislation from (but not limited to) the following:

- Computer Misuse Act 1990
- Data Protection Act 2018
- The UK General Data Protection Regulation (GDPR)
- National Cyber Security Centre: Small Business Guide
- National Cyber Security Centre: Cyber Essentials

This policy should be considered alongside the following documents:

- Compliant Records Management Policy
- Online Safety Policy
- Data Protection Policy
- ICT Acceptable Use Policy
- The Gallery Trust Behaviour and Relationships Policy
- Staff Code of Conduct
- Remote Working and Learning Policy
- Portable Storage Media Policy
- Password and Multi-Factor Authentication Policy

The Gallery Trust's Data Protection Officer (DPO) is Satswana Ltd, info@satswana.com; telephone number 01252 759177.

Section 1 – Exams-related information:

There is a requirement for the exams officer and exams staff in schools to hold exams-related information on candidates taking external examinations. Candidates' exams-related data may be shared with organisations, examination bodies and external verifiers including:

- Awarding bodies
- Joint Council for Qualifications
- Department for Education
- Local Authority
- ASDAN

- NOCN
- Pearson
- WJEC

This data may be shared via one or more of the following methods:

- Hard copy
- Email
- Secure extranet sites (e-AQA, OCR Interchange, Pearson Edexcel online, WJEC Secure services)
- Management Information Systems
- Post to external verifiers

This data may relate to exams entries, coursework, access arrangements, the conduct of exams and non-examination assessments, special consideration requests and exam results/post results/certificate information.

Section 2 – Information for pupils

The Gallery Trust ensures that pupils are aware of the information and data held. All pupils are informed about their examination timetable verbally, and results are shared with pupils and parents/carers by schools. Information about results, assessment and accreditation are provided in reports which may be shared appropriately with third parties by schools (e.g. onward educational establishments, colleges etc). This information can also be included in Education Health and Care Plans.

Pupils receive all their certificates when they leave the school. Copies are not retained, as if necessary, the school can check results of past students through the examination board secure sites.

Section 3 – Dealing with data breaches

Please refer to Appendix 1: Personal Data Breach Procedure in the Data Protection Policy.

Section 4 – Candidate information, audit and protection measures:

All candidates' examination papers will be handled by schools in line with DPA/GDPR guidelines and will be securely retained. Coursework will not necessarily require to be secured, as coursework is part of the everyday requirements of the curriculum, and teaching and learning. Photographs may be taken for assessment use only.

Examination papers are stored securely in archive storage by schools until they are destroyed in line with the Trust's Compliant Records Management policy. Examination papers are stored until the appeals/validation process has been completed, for one year. Examination papers and information containing personal data will be securely destroyed in confidential waste.

Public examination results and internal examination results are added to the pupil's record and securely destroyed by schools at the end of the retention period for pupil records, 25 years after date of birth.

Protection measures for data may include:

- Secure drive accessible only to selected staff
- Information held in secure area
- Updates which apply to the Trust's security measures undertaken regularly (including updating antivirus software, firewalls, internet browsers etc.)
- When sending information through email, e.g. to external verifiers, work is password

protected and the password is sent in a separate email.

Information shared with examination boards and verifiers includes but is not limited to:

- Full name
- Date of Birth
- Gender
- UCI number
- Unique Learning Number
- Assessments
- Coursework
- Results
- Photographs of learners. Photographs are provided for assessment purposes only and are not for publication.

Appendix 3 Social Engineering Awareness

Introduction

In order to fulfil our role as an education provider, The Gallery Trust processes a large amount of data, including personal and sensitive data, on a daily basis. We understand the high risks associated with doing this and, therefore, this protocol has been developed in order to avoid the inappropriate sharing of information. This will form part of the suite of policies designed to ensure compliance with the GDPR.

We are committed to protecting the integrity of data, including preventing it being accessed by social engineers. For this reason, this policy includes definitions and responsibilities that staff need to be aware of to help ensure the security of the Trust's data.

Social Engineering

This is where someone manipulates an individual so that they are coerced into releasing confidential information. There are two types of social engineering – human-based and computer-based; however, both forms are based on the building of inappropriate trust with someone. Criminals use a variety of methods to do this, including via email, telephone and social media.

Phishing

This is the sending of fake emails, texts and phone calls with the aim of gaining people's personal information. Clicking on this kind of email can lead to serious issues, such as identity theft and financial loss for the receiver of the email.

Ransomware

This is a type of malware that prevents or limits individuals from accessing their system and files unless a ransom is paid. A computer can become infected with ransomware when unsecure websites are accessed or a Trojan disguised as a legitimate file is downloaded or opened.

Personal data

This refers to information that relates to an identifiable, living individual, including information such as an online identifier.

Sensitive data

This 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.

1. Roles and responsibilities

The Head of Establishment is responsible for:

- Making staff members aware of this information.
- Ensuring that appropriate security measures are in place, including those in relation to cyber security.
- Making staff members aware of the dangers of social engineering and common techniques used for such attacks.
- Ensuring staff members know how to respond to social engineering attacks.

All staff members are responsible for:

- Acting in accordance with this protocol and the Data Protection Policy at all times.
- Handling data in line with the law and the Trust's Data Handling Procedure.
- Reporting data breaches in line with protocol
- Reporting incidents of social engineering to the Trust DPO, including where this does not result in a data breach.
- Treating personal and sensitive data with the upmost confidentiality at all times.
- Only sharing data with other parties where appropriate to do so.

The Gallery Trust's Data Protection Officer (DPO) is Satswana Ltd, info@satswana.com; telephone number 01252 759177.

2. Methods of social engineering

All staff members will be made aware of the different methods of social engineering which are most commonly used, including:

Human-based:

- Impersonation – this usually involves a social engineer pretending to be an employee, board trustee or technical support in order to gain access to school-specific data, such as employee contact details. This can happen over the phone, in person or via email.
- Third-party authorisation – where a social engineer has obtained the name of someone in the Trust and says that they have been granted access to specific information.
- 'Shoulder surfing' – this is when someone is stood looking over an individual's shoulder whilst they enter data, such as their personal details.

Computer-based:

- Popup windows – this is where a window will appear on the screen, saying e.g. the individual has lost their internet connection and must re-enter their details.
- Mail attachments – viruses can be hidden in email attachments. These are often given names to entice the individual or a long file name.
- Chain, spam and hoax emails – these types of email are often used to gain individual's email addresses and can contain computer viruses.

3. Handling personal data

When handling personal data, staff members will:

- Act in accordance with the Trust's Data Protection Procedure.
- Verify the identity of the person requesting the information before releasing any data.
- Be cautious about communications which involve phrases such as 'urgent matter', 'forgotten password' or 'computer virus emergency'.
- Report to the DPO any form of intimidation for data from 'higher level management' and where the requester is 'name dropping' to give the appearance that they are authorised personnel.

- Verify with the DPO any third-party authorisation before releasing any information.
- Immediately end any communication which they believe to be suspicious and report the communication.
- Be cautious of popup windows, mail attachments and suspicious looking websites, such as those claiming to offer something for free.
- Treat information in the strictest confidence.
- Only share the information on a need-to-know basis.

When handling personal data, staff members will **not**:

- Share the information with an unauthorised individual.
- Release data where the requester's identity cannot be verified.
- Share information which requires releasing information that will reveal passwords, serial numbers, financial data or confidential information.
- Open any emails which they believe to be suspicious.
- Use the Trust's email system to open or send chain letters, as well as spam or hoax emails.
- Enter their personal or sensitive data, such as their password, if someone can view their screen.

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 to the data subject

4. Security measures

Data sharing should be kept to a minimum

Data should be stored on a cloud, and whenever practical only shared by permission to specific individuals using a dedicated link

All digital data will be coded, encrypted or password-protected as appropriate, both on a local hard drive and on a network drive that is regularly backed up off-site.

Memory sticks will not be used.

All hard copies of personal data will be shredded and disposed of: either by shredding immediately or placing in a locked receptacle.

Staff members and students will not download files from unrecognised websites or email senders.

Staff members leaving the Trust will be removed from the Trust's system within an appropriate period to be agreed with line manager. Staff members should be informed of their removal. Staff members transferring to other establishments will retain their access, to be agreed with the Head of Establishment.

All necessary members of staff are provided with their own secure login and password, and every

computer prompts users to change their password in-line with current best practice.

Staff members will not share private information, such as employee contact details and passwords.

Staff working from home must ensure that personal data is retained safely and securely and that no members of their household can access data.

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

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

5. Reporting concerns

If a staff member has a concern, such as not being able to verify the requester's identity, this will be reported to the DPO.

Concerns regarding unsafe emails, computer downloads and the school's filtering system will be reported to the IT technician immediately.

Staff members will be made to feel supported when reporting concerns or violations to this policy.

The Gallery Trust takes its duties under the GDPR seriously and any unauthorised disclosure of data, or intentionally putting the integrity of data in harms way, may result in disciplinary action, in line with the school's Disciplinary Policy and Procedure.

6. Data breaches

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.

If a breach is suspected, please refer to Appendix 1: Personal Data Breach Procedure.