LEARNING OPPORTUNITIES

GDPR and Data Protection Policy

Contents

PAGE NUMBER

The GDPR & Data Protection Policy has been written and approved by a team with a range of experience, and will be reviewed annually.

Previous Review Date: January 2021

Next Review Date: January 2022

Learning Opportunities subscribes to GDPRIS, which provides a comprehensive GDPR Monitoring and Management system to support the school in achieving compliance.

PURPOSE

This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with the Data Protection Act 1998, and other related legislation. It will apply to information regardless of the way it is collected, used, recorded, stored and destroyed, and irrespective of whether it is held in paper files or electronically.

All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities by adhering to these guidelines

INTRODUCTION

Data protection refers to safeguarding private and important information from compromise, corruption, and loss.

Learning Opportunities collects and uses personal information about staff, students, parents / carers and other individuals who come into contact with the school. This information is gathered in order to enable it to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that the school complies with its statutory obligations.

Schools have a duty to be registered, as Data Controllers, with the Information Commissioner's Office (ICO) detailing the information held and its use. These details are then available on the ICO's website. Schools also have a duty to issue a Fair Processing Notice to all students, parents / carers, this summarises the information held on students, why it is held and the other parties to whom it may be passed on.

In accordance with the Data Protection Act 1998, Learning Opportunities has notified the Information Commissioner's Office (ICO) of its processing activities. Learning Opportunities Limited is named as the Data Controller under the Act. Our ICO registration number is **Z7352399**.

This policy relates to all Learning Opportunities staff (including voluntary, temporary and contracted), who capture, create, store, use, share and dispose of information on behalf of Learning Opportunities.

WHAT IS PERSONAL INFORMATION?

Personal information or data is defined as data which relates to a living individual who can be identified from that data, or other information held.

Examples of personal information that a school may store include:

- Names and dates of birth for both staff and pupils.
- Images of staff and pupils that confirm their identity and can be linked to additional personal information.
- National Insurance numbers.

- Addresses of staff and pupils.
- Recruitment information.
- Financial records, such as tax information and bank details.
- Information relating to pupil behaviour and school attendance.
- Medical records, including GP names and medical conditions.
- Exam results and class grades.
- Staff development reviews.
- School assessments and marks.
- Safeguarding information, including data related to SEN assessments.

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 ▪ Health – physical or mental ▪ Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
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.

KEY DATA PROTECTION PRINCIPLES (Refer to Appendix B)

1. Lawfulness, fairness and transparency
Processed lawfully, fairly and in a transparent manner in relation to individuals.

2. Purpose Limitation
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.

3. Data minimisation
Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

4. Accuracy
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.

5. Storage Limitation
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.

6. Integrity and Confidentiality
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

7. Accountability
The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1

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 data protection.

GENERAL STATEMENT

Learning Opportunities is committed to maintaining the above principles at all times. Therefore, the school will:

- Inform individuals why the information is being collected when it is collected
- Inform individuals when their information is shared, and why and with whom it was shared
- Check the quality and the accuracy of the information it holds
- Ensure that information is not retained for longer than is necessary
- Ensure that when obsolete information is destroyed that it is done so
    - appropriately and securely
- Ensure that clear and robust safeguards are in place to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded
- Share information with others only when it is legally appropriate to do so
- Set out procedures to ensure compliance with the duty to respond to requests for access to personal information, known as Subject Access Requests

- Ensure our staff are aware of and understand our policies and procedures

PRIVACY NOTICES

The school will issue privacy notices as required, informing data subjects (or their parents, depending on age of the student, if about student information) about the personal information that it collects and holds relating to individual data subjects, how individuals can expect their personal information to be used and for what purposes.

When information is collected directly from data subjects, including for HR or employment purposes, the data subject shall be given all the information required by the GDPR including the identity of the data controller and the DPO, how and why the School will use, process, disclose, protect and retain that personal data through a privacy notice (which must be presented when the data subject first provides the data).

When information is collected indirectly (for example from a third party or publicly available source) the data subject must be provided with all the information required by the GDPR as soon as possible after collecting or receiving the data. The school must also check that the data was collected by the third party in accordance with the GDPR and on a basis which is consistent with the proposed processing of the personal data.

The School will take appropriate measures to provide information in privacy notices in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

The School will issue a minimum of two privacy notices, one for student information, and one for workforce information, and these will be reviewed in line with any statutory or contractual changes.

INDIVIDUAL RIGHTS

Staff as well as any other 'data subjects' have the following rights in relation to their personal information:

- To be informed about how, why and on what basis that information is processed *(see the relevant privacy notice)*

- To obtain confirmation that personal information is being processed and to obtain access to it and certain other information, by making a subject access request.

- To have data corrected if it is inaccurate or incomplete

- To have data erased if it is no longer necessary for the purpose for which it was originally collected/processed, or if there are no overriding legitimate grounds for the processing ('the right to be forgotten')

- To restrict the processing of personal information where the accuracy of the information is contested, or the processing is unlawful (but you do not want the data to be erased) or where the school no longer need the personal information, but you require the data to establish, exercise or defend a legal claim

- To restrict the processing of personal information temporarily where you do not think it is accurate (and the school are verifying whether it is accurate), or where you have objected to the processing (and the school are considering whether the school's legitimate grounds override your interests)

- In limited circumstances to receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format

- To withdraw consent to processing at any time (if applicable)

- To request a copy of an agreement under which personal data is transferred outside of the EEA.

- To object to decisions based solely on automated processing, including profiling

- To be notified of a data breach which is likely to result in high risk to their rights and obligations

- To make a complaint to the ICO or a Court.

INFORMATION SECURITY

The school will use appropriate technical and organisational measures to keep personal information secure, to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.

All staff are responsible for keeping information secure in accordance with the legislation and must follow their school's acceptable usage policy.

The school will develop, implement and maintain safeguards appropriate to its size, scope and business, its available resources, the amount of personal data that it owns or maintains on behalf of others and identified risks (including use of encryption and pseudonymisation where applicable). It will regularly evaluate and test the effectiveness of those safeguards to ensure security of processing.

Staff must guard against unlawful or unauthorised processing of personal data and against the accidental loss of, or damage to, personal data. Staff must exercise particular care in protecting sensitive personal data from loss and unauthorised access, use or disclosure.

Staff must follow all procedures and technologies put in place to maintain the security of all personal data from the point of collection to the point of destruction. Staff may only transfer personal data to third-party service providers who agree in writing to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

Staff must maintain data security by protecting the **confidentiality, integrity and availability** of the personal data, defined as follows:

Confidentiality means that only people who have a need to know and are authorised to use the personal data can access it.

Integrity means that personal data is accurate and suitable for the purpose for which it is processed.

Availability means that authorised users can access the personal data when they need it for authorised purposes.

Staff must comply with and not attempt to circumvent the administrative, physical and technical safeguards the school has implemented and maintains in accordance with the GDPR and DPA.

Where the school uses external organisations to process personal information on its behalf, additional security arrangements need to be implemented in contracts with those organisations to safeguard the security of personal information. Contracts with external organisations must provide that:

- the organisation may only act on the written instructions of the school
- those processing data are subject to the duty of confidence
- appropriate measures are taken to ensure the security of processing
- sub-contractors are only engaged with the prior consent of the school and under a written contract
- the organisation will assist the school in providing subject access and allowing individuals to exercise their rights in relation to data protection
- the organisation will delete or return all personal information to the school as requested at the end of the contract
- the organisation will submit to audits and inspections, provide the school with whatever information it needs to ensure that they are both meeting their data protection obligations, and tell the school immediately if it does something infringing data protection law.

Before any new agreement involving the processing of personal information by an external organisation is entered into, or an existing agreement is altered, the relevant staff must seek approval from the DPO.

INFORMATION SHARING

Occasionally, we may be required to share personal data with other agencies. On these occasions, it may be the case that actions cannot be completed or verified without sharing such data. For example, if a student shows signs of physical or mental abuse, this information may need to be passed onto social care.

Before sharing this data, all legal implications must be considered. Questions to be considered include:

- Who requires this data?
- Which data is required, and for what purposes will the information be used?
- What is the intention behind sharing this information?

You must also receive consent from any said individual before their personal information is shared. This information should have already been presented in your school privacy notice when the data was initially collected.

Any literature sent from schools to parents / carers requires a printed data protection statement where applicable.

DATA BREACHES

A data breach may take many different forms:

- Loss or theft of data or equipment on which personal information is stored
- Unauthorised access to or use of personal information either by a member of staff or third party
- Loss of data resulting from an equipment or systems (including hardware or software) failure
- Human error, such as accidental deletion or alteration of data
- Unforeseen circumstances, such as a fire or flood
- Deliberate attacks on IT systems, such as hacking, viruses or phishing scams
- Blagging offences where information is obtained by deceiving the organisation which holds it

The school will report a data breach to the Information Commissioner's Office (ICO) without undue delay and where possible within 72 hours, if the breach is likely to result in a risk to the rights and freedoms of individuals. The school must also notify the affected individuals if the breach is likely to result in a high risk to their rights and freedoms.

Staff should ensure they inform the DPO/Head teacher immediately that a data breach is discovered and make all reasonable efforts to recover the information, following the school's agreed breach reporting process.

Actions to minimise the impact of data breaches

We 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. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Below is a list that is not intended to be exhaustive but lists actions we will take for different types of sensitive personal data processed by the school. For example:

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 and the DPO 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 DPO 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, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted

TRAINING

Learning Opportunities will ensure that staff are adequately trained regarding their data protection responsibilities.

CONSEQUENCES OF FAILURE TO COMPLY

Learning Opportunities takes compliance with this policy very seriously. Failure to comply puts data subjects whose personal information is being processed at risk and carries the risk of significant civil and criminal sanctions for the individual and the school and may in some circumstances amount to a criminal offence by the individual.

Any failure to comply with any part of this policy may lead to disciplinary action under the school's procedures and this action may result in dismissal for gross misconduct. If a non-employee breaches this policy, they may have their contract terminated with immediate effect.

If you have any questions or concerns about this policy, you should contact the DPO / Head Teacher.

SCHOOL AUDIT

To guarantee that all information is vetted for accuracy, stored only for the time that it is relevant, and stored securely, annual audits will be carried out. To conduct an audit, we will:

- Monitor all 'live' files to make sure they are updated and accurate.
- Send out a letter at the beginning of each school year urging parents and pupils to check that all of their personal details are correct.
- Amend all information that is inaccurate immediately.
- Destroy all personal data that is no longer needed or out-of-date. This could involve deleting computer files, shredding documents, or formatting hard drives securely so that all information is permanently erased and inaccessible.
- Adhere to the disposal of records schedule, which states the duration that certain types of personal information can be retained before they must be destroyed. Note that some stipulations are legally required while others are recommended for best practice.

DATA PRIVACY IMPACT ASSESSMENTS (DPIA)

A DPIA is a process which helps an organisation to identify and reduce the privacy risks to individuals whose personal information is used in a project. The General Data Protection Regulation (GDPR) will make it a legal requirement to carry out a DPIA where the use of the personal information is likely to result in a high risk to the privacy of individuals

Examples might include use of new technologies, including proposals to use cloud storage facilities for school information.

COMPLAINTS

Complaints will be dealt with in accordance with Learning Opportunities complaints policy. Complaints relating to information handling may be referred to the Information Commissioner (the statutory regulator).

MONITORING & REVIEW

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 2 years. The policy review will be undertaken by the Proprietor, or nominated representative.

CONTACTS

If you have any queries or concerns regarding these policies / procedures, then please contact **Lesley Buss (Proprietor)** lesleyb@learningopps.org **or Simon Graydon (Headteacher)** simong@learningopps.org They will also act as the contact point for any subject access requests.

Further advice and information can be obtained from the Information Commissioner's Office, www.ico.gov.uk or telephone 0303 123 1113

APPENDIX A **GLOSSARY**

Automated Decision-Making (ADM): when a decision is made which is based solely on automated processing (including profiling) which produces legal effects or significantly affects an individual. The GDPR prohibits automated decision-making (unless certain conditions are met) but not automated processing.

Automated Processing: any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. profiling is an example of automated processing.

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

Data Controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. It is responsible for establishing practices and policies in line with the GDPR. The school is the Data Controller of all personal data relating to its pupils, parents and staff.

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

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

Data Protection Officer (DPO): the person required to be appointed in public authorities under the GDPR.

EEA: the 28 countries in the EU, and Iceland, Liechtenstein and Norway.

Explicit Consent: consent which requires a very clear and specific statement (not just action).

General Data Protection Regulation (GDPR): General Data Protection Regulation (*(EU) 2016/679*). Personal data is subject to the legal safeguards specified in the GDPR.

Personal data is any information relating to an identified or identifiable natural person (data subject) who can be identified, directly or indirectly by reference to an identifier such as a name, identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Personal data includes sensitive personal data and pseudonymised personal data but excludes anonymous data or data that has had the

identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

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

Privacy by Design: implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the GDPR.

Privacy Notices: separate notices setting out information that may be provided to Data Subjects when the school collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, school workforce privacy policy) or they may be stand-alone privacy statements covering processing related to a specific purpose.

Processing means anything done with personal data, such as collection, recording, structuring, storage, adaptation or alteration, retrieval, use, disclosure, dissemination or otherwise making available, restriction, erasure or destruction.

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

Pseudonymisation or Pseudonymised: replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.

Sensitive Personal Data: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and Personal data relating to criminal offences and convictions.

Appendix B **KEY PRINCIPLES**

Lawfulness, fairness and transparency

At a glance

- You must identify valid grounds under the GDPR (known as a 'lawful basis') for collecting and using personal data.
- You must ensure that you do not do anything with the data in breach of any other laws.
- You must use personal data in a way that is fair. This means you must not process the data in a way that is unduly detrimental, unexpected or misleading to the individuals concerned.
- You must be clear, open and honest with people from the start about how you will use their personal data.

Checklist

Lawfulness

☐ We have identified an appropriate lawful basis (or bases) for our processing.

☐ If we are processing special category data or criminal offence data, we have identified a condition for processing this type of data.

☐ We don't do anything generally unlawful with personal data.

Fairness

☐ We have considered how the processing may affect the individuals concerned and can justify any adverse impact.

☐ We only handle people's data in ways they would reasonably expect, or we can explain why any unexpected processing is justified.

☐ We do not deceive or mislead people when we collect their personal data.

Transparency

☐ We are open and honest, and comply with the transparency obligations of the right to be informed.

Purpose limitation

At a glance

- You must be clear about what your purposes for processing are from the start.
- You need to record your purposes as part of your documentation obligations and specify them in your privacy information for individuals.
- You can only use the personal data for a new purpose if either this is compatible with your original purpose, you get consent, or you have a clear obligation or function set out in law.

Checklist

☐ We have clearly identified our purpose or purposes for processing.

☐ We have documented those purposes.

☐ We include details of our purposes in our privacy information for individuals.

☐ We regularly review our processing and, where necessary, update our documentation and our privacy information for individuals.

☐ If we plan to use personal data for a new purpose other than a legal obligation or function set out in law, we check that this is compatible with our original purpose or we get specific consent for the new purpose.

Data minimisation

At a glance
You must ensure the personal data you are processing is:

- adequate – sufficient to properly fulfil your stated purpose;
- relevant – has a rational link to that purpose; and
- limited to what is necessary – you do not hold more than you need for that purpose.

Checklist

☐ We only collect personal data we actually need for our specified purposes.

☐ We have sufficient personal data to properly fulfil those purposes.

☐ We periodically review the data we hold, and delete anything we don't need.

Accuracy

At a glance

- You should take all reasonable steps to ensure the personal data you hold is not incorrect or misleading as to any matter of fact.
- You may need to keep the personal data updated, although this will depend on what you are using it for.
- If you discover that personal data is incorrect or misleading, you must take reasonable steps to correct or erase it as soon as possible.
- You must carefully consider any challenges to the accuracy of personal data.

Checklist

☐ We ensure the accuracy of any personal data we create.

☐ We have appropriate processes in place to check the accuracy of the data we collect, and we record the source of that data.

☐ We have a process in place to identify when we need to keep the data updated to properly fulfil our purpose, and we update it as necessary.

☐ If we need to keep a record of a mistake, we clearly identify it as a mistake.

☐ Our records clearly identify any matters of opinion, and where appropriate whose opinion it is and any relevant changes to the underlying facts.

☐ We comply with the individual's right to rectification and carefully consider any challenges to the accuracy of the personal data.

☐ As a matter of good practice, we keep a note of any challenges to the accuracy of the personal data.

Storage limitation

At a glance

- You must not keep personal data for longer than you need it.
- You need to think about – and be able to justify – how long you keep personal data. This will depend on your purposes for holding the data.
- You need a policy setting standard retention periods wherever possible, to comply with documentation requirements.
- You should also periodically review the data you hold, and erase or anonymise it when you no longer need it.
- You must carefully consider any challenges to your retention of data. Individuals have a right to erasure if you no longer need the data.
- You can keep personal data for longer if you are only keeping it for public interest archiving, scientific or historical research, or statistical purposes.

Checklist

☐ We know what personal data we hold and why we need it.

☐ We carefully consider and can justify how long we keep personal data.

☐ We have a policy with standard retention periods where possible, in line with documentation obligations.

☐ We regularly review our information and erase or anonymise personal data when we no longer need it.

☐ We have appropriate processes in place to comply with individuals' requests for erasure under 'the right to be forgotten'.

☐ We clearly identify any personal data that we need to keep for public interest archiving, scientific or historical research, or statistical purposes.

Integrity and confidentiality (security)

You must ensure that you have appropriate security measures in place to protect the personal data you hold. This is the 'integrity and confidentiality' principle of the GDPR – also known as the security principle.

At a glance

- A key principle of the UK GDPR is that you process personal data securely by means of 'appropriate technical and organisational measures' – this is the 'security principle'.
- Doing this requires you to consider things like risk analysis, organisational policies, and physical and technical measures.
- You also have to take into account additional requirements about the security of your processing – and these also apply to data processors.
- You can consider the state of the art and costs of implementation when deciding what measures to take – but they must be appropriate both to your circumstances and the risk your processing poses.
- Where appropriate, you should look to use measures such as pseudonymisation and encryption.
- Your measures must ensure the 'confidentiality, integrity and availability' of your systems and services and the personal data you process within them.
- The measures must also enable you to restore access and availability to personal data in a timely manner in the event of a physical or technical incident.
- You also need to ensure that you have appropriate processes in place to test the effectiveness of your measures, and undertake any required improvements.
- We have worked closely with the National Cyber Security Centre (NCSC) to develop an approach that you can use when assessing the measures that will be appropriate for you.

Checklist

☐ We undertake an analysis of the risks presented by our processing, and use this to assess the appropriate level of security we need to put in place.

☐ When deciding what measures to implement, we take account of the state of the art and costs of implementation.

☐ We have an information security policy (or equivalent) and take steps to make sure the policy is implemented.

☐ Where necessary, we have additional policies and ensure that controls are in place to enforce them.

☐ We make sure that we regularly review our information security policies and measures and, where necessary, improve them.

☐ We have assessed what we need to do by considering the security outcomes we want to achieve.

☐ We have put in place basic technical controls such as those specified by established frameworks like Cyber Essentials.

☐ We understand that we may also need to put other technical measures in place depending on our circumstances and the type of personal data we process.

☐ We use encryption and/or pseudonymisation where it is appropriate to do so.

☐ We understand the requirements of confidentiality, integrity and availability for the personal data we process.

☐ We make sure that we can restore access to personal data in the event of any incidents, such as by establishing an appropriate backup process.

☐ We conduct regular testing and reviews of our measures to ensure they remain effective, and act on the results of those tests where they highlight areas for improvement.

☐ Where appropriate, we implement measures that adhere to an approved code of conduct or certification mechanism.

☐ We ensure that any data processor we use also implements appropriate technical and organisational measures.

Accountability principle

The accountability principle requires you to take responsibility for what you do with personal data and how you comply with the other principles. You must have appropriate measures and records in place to be able to demonstrate your compliance.

At a glance

- Accountability is one of the data protection principles - it makes you responsible for complying with the UK GDPR and says that you must be able to demonstrate your compliance.
- You need to put in place appropriate technical and organisational measures to meet the requirements of accountability.
- There are a number of measures that you can, and in some cases must, take including:
    - adopting and implementing data protection policies;
    - taking a 'data protection by design and default' approach;
    - putting written contracts in place with organisations that process personal data on your behalf;
    - maintaining documentation of your processing activities;
    - implementing appropriate security measures;
    - recording and, where necessary, reporting personal data breaches;
    - carrying out data protection impact assessments for uses of personal data that are likely to result in high risk to individuals' interests;
    - appointing a data protection officer; and
    - adhering to relevant codes of conduct and signing up to certification schemes.
- Accountability obligations are ongoing. You must review and, where necessary, update the measures you put in place.
- If you implement a privacy management framework this can help you embed your accountability measures and create a culture of privacy across your organisation.

- Being accountable can help you to build trust with individuals and may help you mitigate enforcement action.

Checklist

☐ We take responsibility for complying with the UK GDPR, at the highest management level and throughout our organisation.

☐ We keep evidence of the steps we take to comply with the UK GDPR.

We put in place appropriate technical and organisational measures, such as:

☐ adopting and implementing data protection policies (where proportionate);

☐ taking a 'data protection by design and default' approach - putting appropriate data protection measures in place throughout the entire lifecycle of our processing operations;

☐ putting written contracts in place with organisations that process personal data on our behalf;

☐ maintaining documentation of our processing activities;

☐ implementing appropriate security measures;

☐ recording and, where necessary, reporting personal data breaches;

☐ carrying out data protection impact assessments for uses of personal data that are likely to result in high risk to individuals' interests;

☐ appointing a data protection officer (where necessary); and

☐ adhering to relevant codes of conduct and signing up to certification schemes (where possible).

☐ We review and update our accountability measures at appropriate intervals.

APPENDIX C **RETENTION SCHEDULE**

FILE DESCRIPTION	RETENTION PERIOD
Employment Records - covering all employees including temporary workers and those on zero hours, and volunteers (where categories are appropriate)	
Job applications and interview records of unsuccessful candidates	Six months after notifying unsuccessful candidates, unless the school has applicants' consent to keep their CVs for future reference. In this case, application forms will give applicants the opportunity to object to their details being retained
Job applications and interview records of successful candidates	6 years after employment ceases
Written particulars of employment, contracts of employment and changes to terms and conditions	6 years after employment ceases
Right to work documentation including identification documents	2 years after employment ceases
Immigration checks	Two years after the termination of employment
DBS checks and disclosures of criminal records forms	As soon as practicable after the check has been completed and the outcome recorded (i.e. whether it is satisfactory or not) unless in exceptional circumstances (for example to allow for consideration and resolution of any disputes or complaints) in which case, for no longer than 6 months.
Emergency contact details	Destroyed on termination
Personnel and training records (to include code of conduct and other such personnel forms)	While employment continues and up to six years after employment ceases
Annual leave records	Six years after the end of tax year they relate to or possibly longer if leave can be carried over from year to year
Consents for the processing of personal and sensitive data	For as long as the data is being processed and up to 6 years afterwards
Working Time Regulations: ▪ Opt out forms ▪ Records of compliance with WTR	Two years from the date on which they were entered into Two years after the relevant period
Disciplinary and training records	6 years after employment ceases
Allegations of a child protection nature against a member of staff including where the allegation is founded	10 years from the date of the allegation or the person's normal retirement age (whichever is longer). This should be kept under review. Malicious allegations should be removed.
Financial and Payroll Records	
Pension records	12 years
Retirement benefits schemes – notifiable events (for example, relating to incapacity)	6 years from the end of the scheme year in which the event took place
Payroll and wage records	6 years after end of tax year they relate to
Maternity/Adoption/Paternity Leave records	3 years after end of tax year they relate to
Statutory Sick Pay	3 years after the end of the tax year they relate to
Current bank details	No longer than necessary

Financial records (accounts including sales and purchase ledger)	Current year plus 6 years
Sixth Form bursary	Current year plus 3 years
Agreements and Administration Paperwork	
Collective workforce agreements and past agreements that could affect present employees	Permanently
Trade union agreements	10 years after ceasing to be effective
School Development Plans	3 years from the life of the plan
Professional Development Plans	6 years from the life of the plan
Visitors Book and Signing In Sheets	6 years
Instrument of Government	For the life of the school
Meetings schedule	Current year
Governor meeting papers and reports to governors, including hardcopies of signed minutes of FGB meetings & agendas	10 years
Policy documents created and administered by the governing body	Until replaced.
Governor correspondence (sent and received by the governing body)	Current year plus 3 years
Health & Safety Records	
Health and Safety Risk Assessments	3 years from the life of the risk assessment
Any reportable accident, death or injury in connection with work	For at least twelve years from the date the report was made
Accident reporting	Accident book should be retained 3 years after the last entry in the book.
Fire precaution log books	Current year plus 3 years
Medical records and details of: - ▬ control of lead at work ▬ employees exposed to asbestos dust ▬ records specified by the Control of Substances Hazardous to Health Regulations (COSHH)	40 years from the date of the last entry made in the record
Records of tests and examinations of control systems and protection equipment under COSHH	5 years from the date on which the record was made
Temporary and Casual Workers	
Records relating to hours worked and payments made to workers	3 years
Student Records	
Admissions records	Until the child turns 25.
School Meals Registers	Current year plus 3 years
Free School Meals Registers	6 years
Pupil Premium records	Current year plus 6 years.
Pupil Record	Until the child turns 25.
Attendance Registers	3 years from the date of entry
SEN files, reviews and individual education plans	Until the child turns 25.
Other Records	

Emails	3 years unless the contents are required to be kept for a matter relating to any of the previous categories on pages 4-6 in which case, the email would be kept for that retention period (for example, an email relating to an Employee Disciplinary record might be required to be kept for up to 6 years after employment ceases).

APPENDIX D SUBJECT ACCESS REQUESTS

Learning Opportunities procedures for responding to subject access requests made under the Data Protection Act 1998

Rights of access to information

Under the Data Protection Act 1998 any individual has the right to make a request to access the personal information held about them.

These procedures relate to subject access requests made under the Data Protection Act 1998.

Actioning a subject access request

Requests for information must be made in writing; which includes email, and be addressed to Lesley Buss (Proprietor) lesleyb@learningopps.org If the initial request does not clearly identify the information required, then further enquiries will be made.

The identity of the requestor must be established before the disclosure of any information, and checks should also be carried out regarding proof of relationship to the child. Evidence of identity can be established by requesting production of:

- passport
- driving licence
- utility bills with the current address
- Birth / Marriage certificate
- P45/P60
- Credit Card or Mortgage statement

This list is not exhaustive.

Any individual has the right of access to information held about them. However with children, this is dependent upon their capacity to understand (normally age 12 or above) and the nature of the request. The Headteacher should discuss the request with the child and take their views into account when making a decision. A child with competency to understand can refuse to consent to the request for their records. Where the child is not deemed to be competent an individual with parental responsibility or guardian shall make the decision on behalf of the child.

The school may make a charge for the provision of information, dependant upon the following:

- Should the information requested contain the educational record then the amount charged will be dependant upon the number of pages provided.
- Should the information requested be personal information that does not include any information contained within educational records schools can charge up to £10 to provide it.

- If the information requested is only the educational record viewing will be free, but a charge not exceeding the cost of copying the information can be made

The response time for subject access requests, once officially received, is 40 days **(not working or school days but calendar days, irrespective of school holiday periods)**.

However, the 40 days will not commence until after receipt of fees or clarification of information sought

The Data Protection Act 1998 allows exemptions as to the provision of some information; **therefore all information will be reviewed prior to disclosure**.

Third party information is that which has been provided by another, such as the Police, Local Authority, Health Care professional or another school. Before disclosing third party information consent should normally be obtained. There is still a need to adhere to the 40 day statutory timescale.

Any information which may cause serious harm to the physical or mental health or emotional condition of the student or another should not be disclosed, nor should information that would reveal that the child is at risk of abuse, or information relating to court proceedings.

If there are concerns over the disclosure of information then additional advice will be sought.

Where redaction (information blacked out/removed) has taken place then a full copy of the information provided will be retained in order to establish, if a complaint is made, what was redacted and why.

Information disclosed should be clear, thus any codes or technical terms will need to be clarified and explained. If information contained within the disclosure is difficult to read or illegible, then it should be retyped.

Information can be provided at the school with a member of staff on hand to help and explain matters if requested, or provided at face to face handover. The views of the applicant should be taken into account when considering the method of delivery. If postal systems have to be used, then registered/recorded mail must be used.

Complaints

Complaints about the above procedures should be made to the Proprietor who will decide whether it is appropriate for the complaint to be dealt with in accordance with the school's complaint procedure.

Complaints which are not appropriate to be dealt with through the school's complaint procedure can be dealt with by the Information Commissioner. Contact details of both will be provided with the disclosure information.

Learning Opportunities Subject Access Request Form (SAR)

Name of submitting person:

Name of individual who's information is being requested:

Name of authorised authority:

Please provide two appropriate identification types at the time of submitting this form, in person. No personal information will be recorded from your proof of identification. We will not release an individual's personal information until we are satisfied who is raising the request is either the intended recipient or a member of a legitimate authorised organisation (Police, Social Services, Solicitor).

Accepted proofs of identification include:

- Current Passport
- Current Driving License
- Utility bill (less than 3 months old)

Please Complete the Boxes Below

Information Detail Requested	Data Requested	Date Issued

Please note:
Parents/carers or authorities requesting information relating to student's personal data that we process and store will need to submit a Subject Access Request (SAR) form via the school direct.

Adults submitting a SAR may be required to provide more information relating to a request. In these circumstances, we will respond to you within 1 calendar month of submitting this SAR form. However, if any of the information requested is in the educational record, then the school should respond in 15 school days.

Your request may be withheld due to a lawful exemption or where the information might cause serious harm to the physical or mental health of the student or another individual.

APPENDIX E DATA PRIVACY IMPACT ASSESSMENTS (DPIA) (Checklist)

Project name:

Brief description of project.

1. What is the project for? What does it seek to achieve?
2. Will the project collect information about individuals e.g. pupils, parents, staff? If no personal information is collected, a DPIA will not be required.
3. What type of information will it collect? Will it be special category data? e.g. information about an individuals physical or mental health, social care details, details of criminal offences or allegations, or collecting large quantities of personal information? Any of these will raise the level of risk.
4. How will the information be collected? On paper forms? Electronically? Who will have access to this information? How will it be stored and kept secure?

5. How will pupils/staff /parents be made aware of how their personal information is being used? Will a privacy notice be provided? At the end of a paper form? By linking to the school website privacy notice? Does the privacy notice provide sufficient detail about the reasons for collecting the information and who it may be shared with?
6. Do you need consent from the individual to use the information? e.g. because special category data is being collected.
7. Does the project involve the use of new or different technology which could be privacy intrusive e.g. CCTV, monitoring of staff, biometrics, GPS tracking or cloud storage
8. What risks have been identified? What steps have been taken to eliminate or minimise them?
Signature Name (printed) Position Date