**Duty of confidentiality, Data protection and GDPR**

# General Data Protection Regulations (GDPR):

# To uphold the principles of the GDPR legislation:

1. All staff handling personal data are trained according to the company’s data protection policies specified in this e-policy document.
2. All staff will comply with the following when receiving consent for obtaining data;
	* Any requests for consent will be made prominent to the individual and will be separate from the terms and conditions.
	* Staff will allow individuals to make an objection or restriction request by using means including online forms or through emails or conversations.
	* LPP will allow individuals to challenge the accuracy of the data held and will amend data when requests are made.
	* When communicating privacy information to individuals, we will be concise and clear, to the point. The information given will be clearly signposted and will be relevant to the recipient.
3. All staff obtaining or processing personal data will comply with the following procedure, covered by the GDPR:
* All staff are required to document appropriately when acquiring or processing data. The document covers:
	+ Where the data was obtained from:
		- If the data is processed by a third party supplier, a contract will be written, evidenced and signed by all parties to comply with the GDPA and ICO guidance.
	+ How long the personal data is kept:
		- Data obtained through an individual’s consent will be kept on our secure system and reviewed annually.
		- Data obtained through a third party will be kept on our secure system and reviewed every 6 months.
	+ The lawful basis and decision for acquiring and processing the data.
		- The basis of acquiring data is reviewed annually by the dedicated member of staff.
		- The purpose of processing data is reviewed by the dedicated member(s) of staff annually; consent is the most important basis for processing but the 5 other legal bases for processing data may be appropriate to LPP work.
		- If any special category data is acquired, the condition for processing will be documented in accordance with the GDPR.
	+ Where the personal data is held:
		- A reference on the relevant document will be made to allow quick and easy access
	+ Who the data is shared with:
		- Any data shared with a processor will be under legal contract written, evidenced and signed between all parties, covered by the GRPA and ICO guidance.
1. LPP’s policy, covered by the GDPR, for handling personal data request, is as follows any requests made will be recorded in the appropriate documents.
* The timescale given for which staff must complete data requests must not exceed 5 working days of acknowledgement.
* Staff members handling data requests must be trained and competent.
	+ - Any requests that cannot be handled by staff must be passed onto the SDSA’s dedicated Data Protection Officer.
* Staff must record requests for personal data within relevant documents covering:
	+ - When the request was made;
		- When the member of staff became aware of the request;
		- Who made the request (the individual or their legal guardian);
		- What the request was;
		- The member(s) of staff handling the request;
		- How the request was handled.
* Staff will make it known to individuals that their data is held within the SDSA’s secure database and will allow them the option for accessing their data.
	+ - Any data requests received must be given in an appropriate form through a secure system, such as Anycomms+ for schools’ data or encrypted email.
* Staff will acknowledge amendment requests and proceed by:
1. Responding to the initial request and notifying the individual of the process and the timeframe the request will be completed.
2. Making the amendment, recording the date of the change and the staff completing the request.
3. Notifying and confirming with the individual of the change.
4. Notifying any parties that hold the data of this change.
* Staff will acknowledge erasure requests for personal data by:
	+ - 1. Responding to the initial request and notifying the individual of the process and the timeframe the request will be completed.
			2. Erasing all records of the data (including data from any backup systems) and recording the details of the erasure.
			3. Evidencing the details of the request in the relevant documents.
			4. Notifying the individual of the completion of request.
			5. Notifying any parties that hold or process the data of the erasure.
* Staff will acknowledge requests for restrictions to access and processing of personal data by:
	+ - 1. Responding to the initial request by notifying the individual of the process and the timeframe the request will be completed.
			2. Evidencing the changes in the relevant documents.
			3. Notifying the individual of the completion of the request.
			4. Notifying any parties of the request of restriction.
* Individuals must be informed about the impact of their decision to object or restrict data or processing of data. The SDSA may continue, where appropriate, to process data based on legitimate ground outlined with the GDPR legislation.
* Any staff lifting restrictions or objections to data or processing of data must clearly inform the individual(s).
* Staff will acknowledge requests for the transfer or copy of personal data from one IT environment to another in a safe and secure manner by:
	+ - 1. Responding to the initial request by notifying the individual of the process and the timeframe the request will be completed.
			2. Taking the appropriate measures to secure the data, provide the data in a structured, commonly used and machine readable format before fulfilling the request. The data should be easily transferable from IT environment to another without hindrance.
			3. Evidencing the request in the relevant documents.
			4. Notifying the individual of the completion of the request.
			5. Notifying any parties that hold the data of this request.
* Staff will not penalise any individual who wishes to withdraw consent.
* Any requests made verbally will be noted down at the time of receiving, confirmed by the individual and saved in the relevant documents.
* The identity of the requestor must be established before disclosing any information. Checks must be carried out when dealing with the parent(s) or legal guardian(s) of a child. Proof of relationship must be obtained. Staff must evidence any evidence seen.
* If any data has been made public in an online environment, the SDSA will inform other controllers who are protecting the personal data to erase all links to, copies or replications of the data.
1. Ongoing consent will be monitored by trained staff and reviewed on a periodic basis
	* If LPP holds consent that does not meet the GDPR standards we will:
		+ Seek new GDPR-compliant consent;
		+ Identify the lawful basis of processing the data;
		+ Stop processing the data until new consent is acquired.
	* LPP will make privacy information available to individuals and allow them the means of acknowledging their rights to protest.
		+ LPP’s privacy policy will be reviewed annually and kept updated. If any new changes are made, individuals will be informed. This also applies to communicating the privacy policy to children.
		+ Any personal data the LPP holds will be reviewed annually. If the data is obtained through a third party, the data will be reviewed every 6 months.
		+ All contingencies, safeguards and informative services will be kept free of charge to individuals.
	* To implement appropriate technical and organisational measures to integrate data protection into our processing activities, LPP will:
		+ Minimise the amount and type of data we collect, process and store;
		+ Regularly undertake reviews of our public facing documents and policies to ensure we meet the transparency requirements of the GDPR;
		+ Create, review and improve our data security features and control this on an ongoing basis.
	* LPP will review how we ask and record consent on an annual basis.
2. Staff are trained and will comply with the LPP’s policy on handling children’s data and gaining consent.
	* Staff will identify the most appropriate lawful basis of processing children’s data and evidence it in the relevant documents.
	* Staff will verify that the child is over the age of 13 years when asking for their own consent.
		+ Any child under the age of 13 years will need the approval and consent of their parents or a legal guardian.
		+ This does not apply if the service the child is consenting to is for preventative measures or counselling.
	* When requesting consent from children, we will be concise, to the point, easily understood and in plain language. When communicating privacy information, the text will be age appropriate and clearly outline the risks involved in processing and will explain the safeguards we have in place.
	* Any requests made for a child’s information containing data that may cause harm to the physical or mental health of the child will not be disclosed; any information requests that may put the child at risk of abuse or information relating to court proceedings will refused.
3. Data Protection Impact Assessment
	* LPP has carried out a Data Protection Impact Assessment to identify whether any of our processing operations constitute automated decision making with significant effect.
	* LPP will conduct a DPIA annually.
	* Where a DPIA is required, LPP will ensure this is completed and evidenced before starting any projects.
	* All information contained within the DPIA will comply with the requirements under the GDPR and will be detailed in a report.
	* LPP will consult with the ICO where the DPIA indicates the processing of high risks and where the company is unable to mitigate the risks.
4. LPP will manage the information we hold in a secured way so that the management understands the business impact of personal data related risks.
	* LPP have a set security policy and procedures which reflect business objective.
	* We analyse and log any identified threats, vulnerabilities and potential impacts which are associated with our business activities and information.
5. All staff are trained to effectively identify, report and manage data breaches.
	* Data Breaches to personal data must be documented and evidenced in the relevant documents as soon as the member of staff becomes aware. LPP CEO must be informed.
	* Action will be taken to manage and resolve a breach, including a thorough investigation and recovery.
	* If the breach is likely to risk an individual, staff must report the breach to the ICO and the affected individual(s). Breaches must be reported to the ICO within 72 hours of acknowledgement. All breaches must be documented, even if reporting is not necessary.
	* The CEO will monitor the breach type, volume and cost of incident to identify trends and help prevent recurrences.
6. Appropriate persons are appointed to the role of Data Protection Officer and Data Protection Lead for the protection of the company’s data. They must follow the LPP’s approach to data protection and ensure there is a positive working framework and information governance strategy in place to support data protection. The role of the Data Protection Officer is as follows:
	* To support the appointed individual(s) through provision of appropriate training;
	* To ensure there are appropriate means of reporting in place for the individual;
	* To conduct regular data quality checks of LPP’s system and records we hold to review inaccurate records, remove irrelevant data and update records if needed;
	* To provide feedback of any data quality trends to staff members through ongoing awareness campaigns and internal training;
	* To be responsible for data protection compliance and management;
	* To ensure LPP is registered with the ICO;
	* To document and oversee the internal analysis carried out within the company.
7. LPP will deliver training to all staff handling data and encourage personal responsibility and good security behaviours.
	* Regular general awareness campaigns across the company to educate staff of their data protection, security responsibilities and promote data protection and compliance.
	* If and when any changes are made to our company’s policy of procedure, all relevant staff will be informed and training will be provided where necessary.

Staff owe a duty of confidentiality to LPP and its associated partners.

This duty of confidentiality applies both during and after the term of employment and to confidential information relating to LPP. This does not, however, apply to information which has come into the public domain, unless it has come into the public domain through unauthorised disclosure by an employee.

ln particular, staff must:

1. Keep all information confidential unless disclosure of that information is authorised by the company, or it is believed that disclosure is covered by the Public Interest Disclosure Act. The following are examples of what is regarded as confidential information, but these do not constitute an exhaustive list:

* confidential documents of any sort, whether marked confidential or not;
* lists and particulars of LPP customers;
* business methods of LPP.

2. Take all reasonable precautions to avoid unauthorised access to LPP's records, data, and software including that on hardware, floppy disks, magnetic tapes, disks, paper or any other media.

3. Not to disclose any personal codes, or make such access codes available to other staff members or

any other persons unless specifically instructed to do so by the CEO.

4. Not to remove any of the Company's records, data or equipment from the Company's premises without the express consent from the CEO.

5. Dispose of confidential information, whether paper based or not, in a secure manner.

6. Acknowledge that any programme, software design, design improvement, manual, report, etc.,

created, written or invented by a member of staff as part of his/her employment, shall be the property of LPP.

7. On request, and in any event upon termination of employment, no matter how that employment is terminated, return the following items immediately to the Company:

* all documents, procedure manuals or data together with all copies of a confidential nature which are in a staff member's possession or control; and
* all LPP property issued by the Company for a staff member's use.

8. Staff should be aware that they are covered by the Public Interest Disclosure Act 1998 which protects who disclose certain types of information, to certain individuals, in certain circumstances.

A qualifying disclosure is one in which in the reasonable belief of the worker tends to show one or more of the following:

* A criminal offence has been committed, is being committed or is likely to be committed;
* That a person has failed, is failing, or is likely to fail to comply with a particular legal obligation;
* That a miscarriage of justice has occurred, is occurring or is likely to occur;
* That the health and safety of any individual has been, is being, or is likely to be endangered;
* That the environment has been, is being or is likely to be damaged.

The information indicating the occurrence of any of the above has been, is being, or is likely to be deliberately concealed.

* **DPO** - Data Protection Officer
	+ Matt Potts
* **DPL** – Data Protection Lead
	+ Jo Holland

**Internet Use**

Staff are trusted to use the Internet and email facilities responsibly as long as it does not interfere with their work performance. As a general rule, they should use the facilities during work hours solely for the purpose of your work. Excessive use of the internet for personal use and any use of internet to access or hosting of material that may contain images of sexual content, violence, strong language or hate speech, either in or outside of working hours will be considered to be a gross breach of LPP’s disciplinary procedure.

To help protect staff from exposure to inappropriate or illegal material on the internet and to help maintain and audit network security and usage, LPP use internet content filtering and monitoring technology. ln cases of network security breaches and suspected abuse of the internet or IT facilities, LPP will review the logs generated and may share them with third parties such as consultants.

Other unacceptable behaviour that may be considered in gross breach of the company's disciplinary procedure also includes the following:

* Downloading commercial software or any copyrighted materials belonging to third parties, unless this download is covered or permitted under a commercial agreement or other such licence.
* Publishing defamatory and/or knowingly false material about LPP, your colleagues and/or our customers on social networking sites, 'blogs' (online journals), twitch and any online publishing format.
* Undertaking deliberate activities that waste staff effort or networked resources.

**Computer Security**

Staff must ensure that any digital storage media (Disks, USB Drives, CDs/DVDs etc.) used at home or at other locations are checked for viruses before using in conjunction with office machines. Regular virus checks must be made in order to maintain a virus-free system. On detection of a virus, staff should notify either IT Department who will provide assistance with the removal process. Under no circumstances should staff attempt to disable or interfere with the virus scanning software.

IT Equipment and Information stored on it must not be taken away and used for any other purpose other than for business.

Staff are responsible for the security of their passwords which they should not divulge, even to colleagues. Users should change their network password when prompted by the system and other passwords held should be changed on a regular basis.

Users of laptops should store important data in the onedrive folder rather than their local hard drives as hardware faults that may develop could render data as irrecoverable.

Employees failing to comply with the LPP computer security policy may face a disciplinary penalty ranging from a warning to a dismissal.

**Hardware (Laptops, Notebooks, Printers, Modems etc)**

The purchase, installation, configuration and maintenance of computer equipment is the responsibility of LPP and IT service providers.

Computer equipment registers will be maintained to ensure full tracking of IT assets.

The security and safekeeping of portable and other equipment used outsideLPP offices is the responsibility of the member of staff using it. The CEO must be informed in the event of loss of any IT equipment.

**Copyright & licensing**

Staff have a responsibility to ensure that copyright and licensing laws are not breached including when composing or forwarding emails and email attachments. No member of staff is to download software from the internet without express permission especially chat software e.g. MSN Messenger, Screen Savers, peer to peer Downloading and storing (P2P), file sharing software (e.g. Bittorrent/LimeWire).

Downloading unlicensed copyrighted material (e.g. MP3 audio and movies) on any company equipment is also strictly forbidden. LPP allows staff to install software and applications where it is legal to do so and all appropriate licences have been obtained. Unauthorised software or files found on an individual member of staff's computer will be removed and the member of staff may be considered to be in breach of LPP's disciplinary policy.

Computers on the LPP network are periodically and randomly audited on a regular basis to help ensure that unauthorised or unlicensed software is not present.

**Incorrect and poor quality information**

One of the main benefits of the Internet is that it provides access to large amounts of information.

Staff should be aware that in some cases this information is not regulated and they should therefore take extra care to ensure the information they use is accurate and up-to-date.

**Data/Electronic Information**

All employees who deal with personal data have a responsibility under the Data Protection Act to take all possible precautions to protect data against unauthorised loss, destruction or disclosure.

Data management should be in compliance with the Data Protection legislation with regards to data processed within their department. All information/data held on the organisation’s systems is deemed the property of LPP.

Personal/confidential information must be kept secure, be accurate, current and complete.

Appropriate technical measures must be used to safeguard this type of information such as the use of encryption. Care must be taken when taking data off site (for example not leaving a laptop unattended in a vehicle).

**System usage**

Users should ensure their computers are fully shut down and turned off at the end of the day.

Computers should be locked (CTRL + ALT + DEL) or shut down when left unattended for any significant period of time.

Computer users shall not, by any wilful or deliberate act, jeopardise the integrity of the computing equipment, its systems programs or any other stored information to which they have access.

Under the Terms of the Computer Misuse Act (1990), unauthorised access to a computer (sometimes called ''hacking'') or other unauthorised modification to the contents of a computer (such as the deliberate introduction of viruses) are criminal offences punishable by unlimited fines and up to 5 years’ imprisonment.