GDPR Policy for Lowca Community School

Contents

Aims

Our school aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill. This policy applies to all personal data, regardless of whether it is in paper or electronic format.

Legislation and guidance

This policy meets the requirements of the GDPR and the expected provisions of the DPA 2018. It 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 regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

Definitions of Terms

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
- 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.

The data controller, Lowca school processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller. The school is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

Roles and responsibilities- This policy applies to all staff employed by our school, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

Governing board -The governing board has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

Data protection officer- The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable. They will provide an annual report of their activities directly to the governing board and, where relevant, report to the board their advice and recommendations on school data protection issues. The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO. Full details of the DPO's responsibilities are set out in their job description. Our DPO is Carol Ormerod and is contactable via the School Office 01946372656.

Headteacher -The headteacher acts as the representative of the data controller on a day-to-day basis.

All staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address
- Contacting the DPO in the following circumstances: 1) With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure, 2) If they have any concerns that this policy is not being followed , 3) If they are unsure whether or not they have a lawful basis to use personal data in a particular way, 4) 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, 5) If there has been a data breach, 6) Whenever they are engaging in a new activity that may affect the privacy rights of individuals, 7) If they need help with any contracts or sharing personal data with third parties .

Data protection principles

The GDPR is based on data protection principles that our school 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. This policy sets out how the school aims to comply with these principles.

Lawfulness, fairness and transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the school can fulfil a contract with the individual, or the individual has asked the school to take specific steps before entering into a contract
- The data needs to be processed so that the school 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 school, 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 school 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, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018. We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data. If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do 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. This will be done in accordance with the Information and Records Management Society's toolkit for schools.

Sharing personal data

We 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 our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this.
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will: 1) Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law, 2) Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share 3) only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us We will also share personal data with law enforcement and government bodies where we are 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 We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff. Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

Subject access requests and other rights of individuals

Subject access requests Individuals have a right to make a 'subject access request' to gain access to personal information that the school 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
Subject access requests must be submitted in writing, either by letter, email or fax to the DPO.
They should include: 1) Name of individual, 2) Correspondence address, 3) Contact number and email address,4) Details of the information requested. if staff receive a subject access request they must immediately forward it to the DPO.

Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent. Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our school may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis. When responding to requests, we:

• May ask the individual to provide 2 forms of identification
• May contact the individual via phone to confirm the request was made
• Will respond without delay and within 1 month of receipt of the request
• Will provide the information free of charge
• May tell the individual we will comply within 3 months of receipt of the Request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary We will not disclose information if it might cause serious harm to the physical or mental health of the pupil or another individual or 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 or if it is contained in adoption or parental order records or is given to a court in proceedings concerning the child. If the request is unfounded or excessive, we 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. When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

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 we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us 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.

Parental requests to see the educational record

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request.

CCTV

We do not use CCTV in any locations around the school site.

Photographs and videos

As part of our school activities, we may take photographs and record images of individuals within our school. We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. Uses may include within school on notice boards and in school magazines, brochures, newsletters, outside of school by external agencies such as the school photographer, newspapers, and campaigns .Also online on our school website. Consent can be refused or withdrawn at any time. See our photography policy for more information on our use of images.

Data protection by design and default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties.
- 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 Training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of training in the school diary.

We 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. In particular: Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept in a secure office or locked filing cabinet when not in use

- Papers containing confidential personal data must not be left on classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out from the school office
- 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
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- 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 (see our online safety policy / acceptable use agreement/policy on acceptable use])
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected.

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, where we cannot or do not need to rectify or update it. For example, we will shred or incinerate paper-based records, and delete electronic files.

Personal data breaches

The school will make all reasonable endeavours to ensure that there are no personal data breaches. In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1. When appropriate, we will report

the data breach to the ICO within 72 hours. 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

Training

All staff and governors are provided with data protection training as part of their induction process. Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy. This policy will be reviewed and updated if necessary when the Data Protection Bill receives royal assent and becomes law (as the Data Protection Act 2018) – if any changes are made to the bill that affect our school's practice. Otherwise, or from then on, this policy will be reviewed initially in April 2019 and then every 2 years and shared with the full governing board.

Links with other policies this data protection policy is linked to our, Child Protection Policy and Policy for photos and images.

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
- 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: 1) Lost, 2) Stolen, 3) Destroyed, 4) Altered, 5) Disclosed or made available where it should not have been, 6) Made available to unauthorised people
- The DPO will alert the headteacher and the chair of governors
- The DPO will 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: 1) Loss of control over their data, 2) Discrimination , 3) Identify theft or fraud , 4) Financial loss ,5) Unauthorised reversal of pseudonymisation (for example, key-coding) 6) Damage to reputation , 7) Loss of confidentiality , 8) Any other significant economic or social disadvantage to the individual(s) concerned. If it's 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 stored on the school's computer system. • Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website 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, 2) The categories and approximate number of personal data records concerned, 3) The name and contact details of the DPO, 4) A description of the likely consequences of the personal data breach, 5) 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 on the school's computer system. The DPO and head teacher 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

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. 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 System IT 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 Other types of breach which may occur could include: Details of pupil premium interventions for named children being published on the school website. Recall the information as soon as you become aware of the error. Report the error to the DPO who will take necessary action Non-anonymised pupil exam results or staff pay information being shared with governors. If special category data (sensitive information) is accidentally made available to governors, the information should be recalled as soon as the error is realized. Governors who receive pupil exam results or staff pay information 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 information for any reason, the DPO take necessary action. In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the information, 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 and deleted if a school laptop containing non-encrypted sensitive personal data being stolen or hacked. If a school laptop or pen drive containing non-encrypted sensitive personal

information is stolen or hacked the owner of the laptop/ pen drive must report it to the DPO as soon as they become aware of the loss/ hack. 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 comply with procedures set out in Appendix 1 – Personal Data Breach Information The school's cashless payment provider being hacked and parents' financial details stolen. If Orian's cashless payment system is being hacked and parent's financial details are stolen the incident will be reported to the DPO and Orian as soon as they become aware of the incident. The DPO will liaise with Orian's DPO. 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 comply with procedures set out in the Personal Data Breach Information as described earlier.

Signed 12 12 19 on behalf of governing body
Next review Dec 2020