

# Ukraine Aid and Welfare School GDPR policy

Last review completed by	William Maude-Roxby
Date of last review	April 2024
Next review due	April 2025
Approved by Board	April 2024

## DATA PROTECTION POLICY

### 1 Scope

The Ukrainian school aims to ensure that all personal data collected about staff, pupils, parents, governors, directors, members, visitors, and other individuals is collected, stored, and processed in accordance with UK Data Protection law.

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

### 2 Legislation and guidance

This policy meets the requirements of the UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2020 and the Data Protection Act 2018 (DPA 2018). It is based on guidance published by the Information Commissioner’s Office (ICO) on the GDPR.

### 3 Definitions

#### Term Definition

Personal data - Any information relating to an identified, or identifiable, living 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, organizing, 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 organization 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, unauthorized disclosure of, or access to, personal data.

## **5 Roles and responsibilities**

This policy applies to all staff employed by the Ukrainian School, and to external organizations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action. Further information for staff is set out in our Code of Conduct.

### **5.1 Board of Directors**

The Board of Directors has overall responsibility for ensuring that the Ukrainian school complies with all relevant data protection obligations.

### **5.2 Headteachers**

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

### **5.3 All staff**

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 Headteacher in the following circumstances:
  - o With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
  - o If they have any concerns that this policy is not being followed
  - o If they are unsure whether or not they have a lawful basis to use personal data in a particular way
  - o 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 UK
  - o If there has been a data breach
  - o Whenever they are engaging in a new activity that may affect the privacy rights of individuals
  - o If they need help with any contracts or sharing personal data with third parties

## **6 Data protection principles**

UK GDPR is based on data protection principles that the Ukrainian 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 Ukrainian school aims to comply with these principles.

## **7 Collecting personal data**

### **7.1 Lawfulness, fairness, and transparency**

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under UK 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 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 or another person i.e., 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 or exercise its official authority
- The data needs to be processed for the legitimate interests of the school (where the processing is not for any tasks the school performs as a public authority) 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 under data protection law:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given explicit consent
- The data needs to be processed to perform or exercise obligations or rights in relation to employment, social security, or social protection law
- The data needs to be processed to ensure the vital interests of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made manifestly public by the individual
- The data needs to be processed for the establishment, exercise, or defense of legal claims
- The data needs to be processed for reasons of substantial public interest as defined in legislation
- The data needs to be processed for health or social care purposes, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law
- The data needs to be processed for public health reasons, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law
- The data needs to be processed for archiving purposes, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest

For criminal offence data, we will meet both a lawful basis and a condition set out under data protection law. Conditions include:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given consent
- The data needs to be processed to ensure the vital interests of the individual or another person,

where the individual is physically or legally incapable of giving consent - The data has already been made manifestly public by the individual

- The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of legal rights

- The data needs to be processed for reasons of substantial public interest as defined in legislation

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

We will always consider the fairness of our data processing. We will ensure we do not manage personal data in ways that individuals would not reasonably expect or use personal data in ways which have unjustified adverse effects on them.

## **7.2 Limitation, minimization, and accuracy**

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 to do their jobs.

We will keep data accurate and, where necessary, up to date. Inaccurate data will be rectified or erased when appropriate.

In addition, when staff no longer need the personal data they hold, they must ensure it is deleted or anonymized. This will be done in accordance with the Trust's record retention schedule.

## **8 Sharing personal data**

We will not normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. These include, but are not limited to, situations where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to consult 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 (such as our IT provider). When doing this, we will:
  - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
  - Establish a contract with the supplier or contractor to ensure the fair and lawful processing of any personal data we share
  - Only share data that the supplier or contractor needs to conduct their service

We will also share personal data with law enforcement and government bodies where we are legally required to do so.

We may also share personal data with emergency services and local authorities to help them to respond to an emergency that affects any of our pupils or staff.

Where we transfer personal data internationally, we will do so in accordance with UK data protection law.

## **9 Subject access requests and other rights of individuals**

### **9.1 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 is not possible, the criteria used to determine this period
  - Where relevant, the existence of the right to request rectification, erasure, or restriction, or to object to such processing
  - The right to lodge a complaint with the ICO or another supervisory authority
  - 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 - The safeguards provided if the data is being transferred internationally
- Subject access requests can be submitted in any form, but we may be able to respond to requests more quickly if they are made in writing and include:
- Name of individual
  - Correspondence address
  - Contact number and email address
  - Details of the information requested

If staff receive a subject access request in any form, they must immediately forward it to their Headteacher.

## **9.2 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 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 schools 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.

## **9.3 Responding to subject access requests**

When responding to requests, we:

- May ask the individual to provide two 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 (or receipt of the additional information needed to confirm identity, where relevant).
- 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 may not disclose information for a variety of reasons, such as if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual;
- Would reveal that the child is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the child's best interests.
- Would include another person's personal data that we can't reasonably anonymize, and we don't have the other person's consent and it would be unreasonable to proceed without it;
- Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts.

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee to cover administrative costs. We will take into account whether the request is repetitive in nature when making this decision.

## **9.4 Other data protection rights of the individual**

In addition to the right to make a subject access request (see above), and to receive information when 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 (in certain circumstances).
- Prevent use of their personal data for direct marketing.
- Object to processing which has been justified based on public interest, official authority, or legitimate interests.
- Challenge decisions based solely on automated decision making or profiling (i.e., making decisions or evaluating certain things about an individual based on their personal data with no human involvement).
- Be notified of a data breach (in certain circumstances).
- Ask for their personal data to be transferred to a third party in a structured, commonly used, and machine-readable format (in certain circumstances).

## **10 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. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

Any photographs and videos taken by parents/carers at school events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers have agreed to this.

Where the school takes photographs and videos, uses may include:

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

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

Permission will be sought from parents as part of the school admissions process and parents will be offered the opportunity to update their preferences periodically.

## **12 Data protection by design and default**

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

- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6).
- Completing data protection impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies
- Integrating data protection into internal documents including this policy, any related policies and privacy notices.
- Regularly 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 attendance.

- Regularly conducting reviews and audits to evaluate our privacy measures and make sure we are compliant.
- Appropriate safeguards being put in place if we transfer any personal data outside of the UK, where different data protection laws will apply.
- Maintaining records of our processing activities, including:
  - For the benefit of data subjects, making available the name and contact details of our school and all information we are required to share about how we use and process their personal data (via our privacy notices).
  - For all personal data that we hold, maintaining an internal record of the type of data, type of data subject, how and why we are using the data, any third-party recipients, any transfers outside of the UK and the safeguards for those, retention periods and how we are keeping the data secure.

### **13 Data security and storage of records**

We will protect personal data and keep it safe from unauthorized 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 under lock and key when not in use.
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, 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 10 characters long containing letters and numbers are used to access school computers, laptops, and other electronic devices. Staff and pupils are reminded that they should not reuse passwords from other sites.
- Encryption software is used to protect all portable devices such as laptops.
- Where we need to share personal data with a third party, we conduct due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8).

### **14 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 overwrite or delete electronic files.

We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

### **15 Personal data breaches**

The School will make all reasonable endeavors 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. Such breaches in a school context may include, but are not limited to:

- Safeguarding information being made available to an unauthorized person
- The theft of a school laptop containing non-encrypted personal data about pupils

### **16 Training**

All staff, governors and directors are provided with data protection training as part of their induction process and on an ongoing basis via briefings and specific training. Data protection will also form part of continuing professional development, where changes to legislation, guidance or the School's processes make it necessary.

## **17 Monitoring arrangements**

The Headteacher is responsible for monitoring and reviewing this policy. This policy will be reviewed at least every two years and approved by the Board of Directors.

## **18 Links with other policies**

This Data Protection policy is linked to our:

- Freedom of information publication scheme
- Records management policy
- E-safety – please see individual school policy
- Code of conduct
- ICT usage policy
- Social media policy
- Child protection policy

## **Appendix 1: Personal data breach procedure**

1. On finding or causing a breach, or potential breach, the staff member, governor, member, director, or data processor must immediately notify the Headteacher by using the email address.
2. The school will investigate the report and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
  - Lost
  - Stolen
  - Destroyed
  - Altered
  - Disclosed or made available where it should not have been
  - Made available to unauthorized people
3. Staff, governors, directors, and members will cooperate with the investigation (including allowing access to information and responding to questions). The investigation will not be treated as disciplinary investigation.
4. If a breach has occurred or it is likely that is the case, the school will alert the Chair of the Board of Directors.
5. The school will make all reasonable efforts to contain and minimize the impact of the breach. Relevant staff members or data processors should help the school with this where necessary, and should the school take external advice when required (e.g., from IT providers).
6. The school will assess the potential consequences, based on how serious they are, and how likely they are to happen before and after the implementation of steps to mitigate the consequences.

As required, the school will set out:

- A description of the nature of the personal data breach including, where possible:
- The categories and approximate number of individuals concerned
- The categories and approximate number of personal data records concerned
- The name and contact details of the school
- A description of the consequences of the personal data breach

- A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned.
- 7. If all the above details are not yet known, the school will report as much as they can within 72 hours of the school's awareness of the breach. The report will explain that there is a delay, the reasons why, and when the school expects to have further information. The school will submit the remaining information as soon as possible.
- 8. Where the School is required to communicate with individuals whose personal data has been breached, the school will tell them in writing. This notification will set out:
  - A description, in clear and plain language, of the nature of the personal data breach
  - The name and contact details of the school
  - A description of the 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
- 9. The school will consider, considering the investigation and any engagement with affected individuals, whether to notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks, or credit card companies.
- 10. The school will document 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)
- 11. Records of all breaches will be stored by each school on a spreadsheet on the school's computer system for that purpose.
- 15. The school and Headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.
- 16. The school and Headteachers will meet annually to assess recorded data breaches and identify any trends or patterns requiring action by the school to reduce risks of future breaches.

### **Actions to minimize the impact of data breaches**

We set out below the steps we might take to try and mitigate the impact of data breaches, particularly of risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Should sensitive information be disclosed via email (including safeguarding records):

1. If special category data (sensitive information) is accidentally made available via email to unauthorized individuals, the sender must attempt to recall the email as soon as they become aware of the error.
2. Members of staff who receive personal data sent in error must alert the sender and the school as soon as they become aware of the error.
3. If the sender is unavailable or cannot recall the email for any reason, the school will ask the IT support provider to attempt to recall it from external recipients and remove it from the school's email system (retaining a copy if required as evidence).
4. In any cases where the recall is unsuccessful or cannot be confirmed as successful, the school will consider whether it's appropriate to contact the relevant unauthorized 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.
5. The school will endeavor to obtain a written response from all the individuals who received the data, confirming that they have complied with this request.
6. The school will conduct 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.

7. If safeguarding information is compromised, the school will inform the relevant Designated Safeguarding Lead and discuss whether the school should inform any, or all, of its local safeguarding partners.