DATA PROTECTION POLICY

Crown International Guardians Ltd. (hereinafter called Crown International Guardians) is committed to protecting the privacy of staff, volunteers, clients and supporters under the new General Data Protection Regulation (GDPR) (May 2018). Crown International Guardians is registered with the Information Commissioners Office (ICO), which is the UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

1. Personal Data

This is any personal data you share with us, and could include: your name, your postal address, your email address and your telephone number. This may be used for the following purposes:

- to respond to your queries;
- to provide services where requested;
- to keep you informed about our work, news and campaigns and fundraising;
- to measure trends in the visitors to our website and to improve the web experience for our visitors.

You have the right to request to see, amend or remove any personal information we hold about you. See section **2: Your Rights** below.

Confidentiality and data protection

We do not sell or swap your details with any third parties. If further services are required your explicit consent will be required before being actioned. We are committed to ensuring that your information is secure. In order to prevent unauthorised access or disclosure, we have put in place suitable physical, electronic and managerial procedures to safeguard and secure the information we collect. This includes designated Data Controller/s who are responsible for the safeguarding of your personal data.

Crown International Guardians may need to share contact details with the AEGIS office and lead and supporting inspectors for the purposes of a (re)accreditation inspection.

Storing your data

Our office is completely paperless. Any physical documents that arrive are scanned into our network storage and the originals are shredded immediately.

Any original documents that need to be returned to their owner are sent on the day of receipt. If the post collection has been missed, then they are securely stored until the next working day.

All scanned documents are stored in our dedicated servers.

Any other information not stored in the form of a document image eg. information given during online application, is stored in our database.

All hardware is owned, maintained and managed by Crown International Guardians.

Security precautions in place to protect the loss, misuse or alteration of your information

Non-sensitive details (your email address etc.) are transmitted normally over the Internet, and this can never be guaranteed to be 100% secure. As a result, while we strive to protect your personal information, we cannot guarantee the security of any information you transmit to us, and you do so at your own risk.

Information is held by PC, with relevant safeguards in place using password protection and Anti-Virus and Malware protection and two factor authentication.

Cloud backup is used to back up the devices and stored with major providers. Secure file sharing is used to various devices with a major provider.

Legal basis (or bases)

The legal bases on which we process your data are as follows:

- The data needs to be processed so that Crown International Guardians can fulfil a contract with the individual, or the individual has asked Crown International Guardians to take specific steps before entering into a contract
- The data needs to be processed so that Crown International Guardians can comply with a contractual 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 Crown International Guardians can perform a task carry out its functions
- The data needs to be processed for the legitimate interests of Crown International Guardians 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

Special category data

There are various types of special category data which Crown International Guardians will store and process. These include:

- Personal data relating to minors, such as email, telephone number. This information is required in order to ensure such minors are protected.
- Data relating to ethnicity.
- Medical information. Without such information we cannot ensure medication is administered correctly, and to provide background should a medical necessity arise.

Links to other websites

Our website may contain links to other websites of interest. However, once you have used these links to leave our site, you should note that we do not have any control over that other website. Therefore, we cannot be responsible for the protection and privacy of any information which you provide whilst visiting such sites and such sites are not governed by this privacy statement. You should exercise caution and look at the privacy statement applicable to the website in question.

Breach Notification

A personal data breach may mean that someone other than the data controller gains unauthorised access to personal data. However, a personal data breach can also occur if there is unauthorised access within an organisation, or if a data controller's own employee accidentally alters or deletes personal data.

Crown International Guardians will make all reasonable endeavours to ensure personal data is protected and there are no data breaches. In the unlikely event of a data breach or a suspected data breach, Crown International Guardians will follow the procedure set out in our Data Breach Procedure.

When appropriate, the DPO will report the data breach to the ICO within 72 hours. Such breaches, in a school context, may include, but are not limited to:

- Safeguarding information being made available to an unauthorised person
- The theft of a school device containing non-encrypted personal data

All breaches of the GDPR are to be reported without undue delay to the Information Commissioners Office (ICO) within 72 hours, unless the breach is unlikely to result in any risk to the rights and freedoms of data subjects, and to the data subjects without undue delay unless a specified exemption applies.

Notifications to the data subjects will provide name and contact details of the data controller where more information can be obtained, the likely consequences of the personal data breach and the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

DATA BREACH PROCEDURE

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

1. On finding a breach or potential breach, Crown International Guardians or data processor must immediately notify the DPO.

2. The DPO will undertake an initial investigation to determine whether a breach has occurred. He will consider whether personal data has been accidentally or unlawfully:

   - Altered
   - Destroyed
   - Lost
   - Published or made available to an inappropriate audience
   - Stolen
   - Made available to unauthorised people

3. The DPO is to brief Crown International Guardians Director.

4. 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.

5. The DPO will decide if the breach must be reported to the ICO. This will be judged on a case-by-case basis. The DPO is to take into consideration whether the breach is likely to negatively affect people's rights and freedoms, cause them any physical, material or non-material damage (e.g. emotional distress) through:

   - Damage to reputation
   - Discrimination
   - Financial loss
   - Identify theft or fraud
   - Loss of confidentiality
   - Loss of control over their data
   - Unauthorised reversal of pseudonymisation (for example, key-coding)

- Any other significant economic or social disadvantage to the individual(s) concerned

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

6. The DPO will document the decision (either way), in case it is challenged later by the ICO or an individual affected by the breach. Documented decisions are stored in a spreadsheet on Bright World's computer network.

7. Where the ICO must be notified, the DPO will complete the 'report a breach' page on the ICO's website within 72 hours. As required, the DPO will set out:

a. 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

b. The name and contact details of the DPO.

c. A description of the likely consequences of the personal data breach.

d. 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 he can within the 72 hours timeframe. The report will explain 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.

8. 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:

a. The name and contact details of the DPO

b. A description of the likely consequences of the personal data breach

c. 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 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.

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

a. Facts and cause

b. Effects

c. Action taken to contain it and ensure it does not happen again (such as establishing more robust processes

or providing further training for individuals)

d. Records of all breaches will be stored spreadsheet on Crown International Guardians' computer network

11. The DPO and board will meet to review the breach and lessons learnt. This meeting will happen as soon as reasonably practicable.

2. Your Rights

Data Subject Rights and Subject Access Requests

Crown International Guardians is fully committed to respecting individuals' rights to access personal information held about them in accordance with Article 17 of the GDPR.

Subject access rights

Any individual who makes a valid subject access request is entitled to be:

- The right to request a copy of the personal information held about them
- The right to request that inaccurate or incomplete information about them is rectified
- The right to request that their personal information is deleted
- The right to request that the processing of their personal information is restricted
- The right to data portability
- The right to object to the processing of their information
- The right to complain to the ICO if they are not happy with how their personal information has been processed, or they feel their data protection rights have been infringed.

Individuals are only entitled to their own personal data, and not to information relating to other people, unless they are acting on behalf of that person. In these circumstances, written consent will be required.

Exempt information

Crown International Guardians may not be able to release some information. Information which is exempt from a subject access request includes:

- personal data where disclosure could prejudice the prevention or detection of crime; and,
- personal data identifying another person (a third party) whose details cannot be disclosed without their permission.

How to make a request

In order to make a valid subject access request the following must be provided:

- a clear written request by letter or email.

Proof of identification may be requested to ensure that the personal information requested is provided to the right person. Two forms of ID will be required. One must be name identification (e.g. Driving Licence, Passport or Birth Certificate) and the other a form of address identification dated in the last three months.

Retention period of information

For students and their parents, our retention period is the length of time a student is under our guardianship plus 7 years from leaving as all records are integrated within our accounts information.

After 7 years of inactivity, the data held for students and their parents is automatically deleted.

Crown International Guardians will comply with requests for access to personal information within one month, as required by the Act. All subject access requests should be addressed to:

Mr Alan MacRae (Data Controller),
Crown International Guardians Ltd.
Rickford Mill,
Leg Lane,
Rickford,
BS40 7AH

Email:

mail@crowninternationalguardians.co.uk / alan.macrae.01@gmail.com

Changes to this policy

Crown International Guardians reserves the right to make any changes to this Privacy and Data Protection Policy, and other aspects of this site at any time. Please check this page regularly for any changes.

Policy updated: 29/12/2025 **Policy review date:** 29/12/2026