Information Governance Policy

1. The purpose of this policy is to protect patient and donor data by ensuring that Gateshead Hatzola (Hatzola) complies with the requirements of the General Data Protection Regulation (GDPR), the Data Protection Act 2018 and other relevant legislation and guidance as well as the regulations set by the Care Quality Commission:

- Health and Social Care Act 2008 (Regulated Activities) Regulations 2014: Regulation 17: Good governance

2. This policy takes account of Article 5 of the GDPR which specifies that data must be:

    - processed lawfully, fairly and in a transparent manner in relation to individuals;
    - 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;
    - adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
    - 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;
    - 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; and
    - 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.

3. The Nominated Individual is the Data Controller. Volunteers, staff and contractors, where they exist, are Data Processors.

4. The Nominated Individual or his deputy is responsible for ensuring that data protection principles are followed.

5. All volunteers, employees and contractors are responsible for ensuring the security of data and will receive appropriate training or instructions.

6. Hatzola holds and processes three types of data:

    - patient data
    - donor data

- volunteer or employee data

7. The lawful bases for Hatzola to process data are:

    - legal obligation, to comply with the requirements of the Health and Social Care Act 2008 (Regulated Activities) Regulations 2014: Regulations 17 and 18 and the Safeguarding Vulnerable Groups Act 2006;
    - vital interests, to record contact and health data which may contribute to saving a patient's life in a medical emergency; and
    - legitimate interests, to improve patient outcomes by holding and sharing health information with other health agencies and by clinical audit to improve its service and to support fundraising by maintaining records of donors.

8. Hatzola holds and processes the following personal information:

    - name
    - address
    - telephone number
    - gender
    - date of birth or age
    - Disclosure and Barring Service certificate numbers
    - bank account details

    and the following special category information:

    - health, including injuries, medical conditions, medication and treatment provided

9. Personal information, including special category information, may be held in the following forms:

    - operator report forms – paper and electronic
    - patient report forms – paper and electronic
    - electronic recordings of telephone calls
    - electronic recordings of radio traffic
    - databases or spreadsheets containing extracts from all of the above
    - single central register of volunteers and staff - electronic
    - donor records – paper and electronic, including copies of standing order mandates, Gift Aid declarations and data received from companies processing donations
    - emails received via the Hatzola website.

10. Hatzola will not collect data on visitors to its website other than that provided by companies processing donations made via the website or that provided explicitly on the contact page.

11. All reasonable precautions must be taken to ensure the security of data. This includes, but is not limited to:

- electronic data must be held in encrypted files or on encrypted media
- data which is held online will be stored only on sites which comply with UK data protection legislation and will be protected by suitable passwords. Access rights will be limited to the minimum required for processing the data.
- an appropriate backup regime must be followed for all electronic data
- physical data must be held in locked containers within locked premises, must only be removed for processing and must be replaced immediately after use
- physical data which is no longer required must be disposed of as soon as possible by secure shredding
- electronic data which is no longer required must be securely deleted as soon as possible
- completed patient report forms and operator report forms must be forwarded for recording at the earliest possible opportunity and must not be held by individual volunteers for longer than necessary
- volunteers must ensure that no unauthorised persons have access to report forms while they are in their possession
- patient data being emailed must only be sent between secure email addresses or must be encrypted with the password transferred by another means
- volunteers, employees or contractors must not hold patient data on their personal electronic devices without specific permission from the Co-ordinator or his deputy and must securely delete it as soon as it is no longer required
- volunteers, employees or contractors must not post any patient information on social media, even if anonymised, without specific permission from the Co-ordinator or his deputy

12. Any volunteer, employee or contractor who becomes aware of a data breach must immediately report this to the Nominated Individual or his deputy, who will conduct an investigation and report it to the Information Commissioner's Office within 72 hours if there is a risk of an adverse effect on people's rights or freedoms. In all events, a full internal record will be maintained of the breach and the precautions taken to prevent a recurrence.

13. Personal information will not be hold for longer than necessary and will be securely destroyed or erased at the end of the retention period, except where it is necessary to retain it because of on-going regulatory or legal proceedings, in which case it will be erased as soon as possible after these are completed.

- Patient data will be retained for 10 years or 10 years after the patient's 18th birthday in the case of a patient under 18 years of age.
- Donor data will be retained for 6 years after the last donation is received.
- Volunteer data will be retained for 1 year after the volunteer has ceased to volunteer for Hatzola.
- Employee data will be retained for 6 years after the employee has ceased to be employed by Hatzola.

- Website contact data will be retained for 1 year after the enquiry or request has been dealt with.

14. Personal information, including special category information where appropriate, may be shared with:

    - other agencies and professionals in the interests of patient care
    - the police in the interests of crime prevention and detection
    - social services and other relevant agencies in order to safeguard children and vulnerable adults
    - the Disclosure and Barring Service in order to carry out required checks on volunteers and staff
    - HMRC in order to process Gift Aid claims and if required to assist with their investigations
    - the Care Quality Commission to enable them to carry out statutory functions
    - donors' banks to enable them to process standing orders

    and within Hatzola for quality improvement and training purposes, when it will be anonymised if possible.

15. Individuals on whom information is held have a right to request confirmation of its existence and a copy of that information. This will normally be provided free of charge and within 30 days of the request being received in writing or by email, once the identity of the individual has been confirmed. A fee may be charged to reflect the administrative costs of responding to a complex or repeated request.

16. Information will not be provided if:

    - it is likely, in the opinion of Hatzola's Clinical Director or another qualified medical professional, to be detrimental to the physical or mental health of the individual or any other person
    - it may prejudice a criminal or safeguarding investigation
    - the request is manifestly unfounded, excessive or repetitive.

    In such a case, the individual will be informed in writing within 30 days of the decision and of their right to complain to the Information Commissioner or to request a judicial review.

17. A young person over the age of 13 who is deemed by the Nominated Individual or his deputy to be competent is entitled to request copies of their own information. In all cases, a young person shall be deemed to be competent from 16 years of age. Parents may make a request for their child's data where the child is below 16 years of age, subject to clause 16.

18. Where information is being held for fundraising purposes, an individual may request that their data be erased. This must be carried out within 30 days and confirmed in writing, save where it is necessary to comply with financial reporting requirements, in which case it must be erased at the earliest opportunity.

19. If a volunteer or employee who has left Hatzola requests that their data be erased, this must be done within 30 days, save where it is required to be retained to comply with relevant legislation, in which case it must be erased at the earliest opportunity.

20. This policy will be reviewed by the trustees every two years or when legislation changes.

Author	M Glickman
Adopted	May 2018 – v1
Revised	October 2018 – v2
Revised	February 2020 – v3
Revised	May 2021 – v4
Reviewed by trustees	June 2023
Review due	June 2025