Confidentiality and Data Protection Policy

Nova recognises the right of individuals to confidentiality and that they have a right to expect that personal details will be kept confidentially and in line with the requirements of law.
Nova recognises that misuse of data can be damaging and distressing and is committed to but not limited by the principles of the **UK General Data Protection Regulation (UK GDPR)**, the **Data Protection Act 2018 (DPA 2018)**, and the **Privacy and Electronic Communications Regulations 2003 (PECR)** (the **Data (Use and Access) Act 2025 (DUAA)** has made some targeted amendments, but doesn't replace the core legislation) which provide individuals with protection from unwanted or harmful use of data.
Nova also believes that the right to privacy, confidentiality and appropriate use of data are essential to ensure all individuals have full confidence in the organisation and are treated with respect and dignity.

Data Protection

All staff are expected to abide by the regulations set out in the Data Protection Act regarding the storage of personal data on individuals. Under the Data Protection Act 2018 we have responsibilities regarding the data and information we hold on individuals. It is necessary for the organisation to collect personal data and other information about an individual in order for it to carry out its functions as a service provider, fundraising organisation, employer and provider of volunteering opportunities.

Accordingly, we need to comply with certain principles regarding data:

- Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless certain conditions are met.
- Personal data shall be obtained only for one or more specified and lawful purpose and shall not be further processed in any manner incompatible with that purpose or those purposes.
- Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
- Personal data shall be accurate and, where necessary, kept up to date.
- Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
- Personal data shall be processed in accordance with the rights of data subjects under the Act.
- Data should be kept secure and appropriate technical and organisation measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
- The cloud provider must comply with UK data protection laws. A written contract must be in place that outlines their responsibilities as a data processor.

- Personal data shall not be transferred to a country of territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

- Maintaining detailed records of your processing activities (known as a **Record of Processing Activities** or ROPA).

All Nova employees and volunteers must ensure that they work in accordance with these principles. The CEO can provide you with further information on the Data Protection Act 2018 and its implications.

Data management

The Head of Impact Measurement and Compliance is Nova's designated Data Controller who oversees data management in consultation with the CEO.

Responsibilities

The Data Controller is responsible for ensuring that all staff and volunteers at Nova are aware of the legal and policy restrictions placed upon holding and processing personal data; that personnel comply with these requirements; and that personal data is held in accordance with the Nova's Notification under the Data Protection Act.

Workers have a legal right to access information that an employer may hold on them. This could include information regarding any grievances or disciplinary action, or information obtained through monitoring processes. If requested, a 40-day time limit is stipulated for response. Information can be withheld if releasing it would make it more difficult to detect crime or the information is about national security. If an employee feels the organisation has misused information or hasn't kept it secure, they can contact the Information Commissioner's Office.

Physical security

Nova's servers are located in a designated server room. Access to this room is limited to personnel authorised by the Network Administrator. The room must be kept locked when unoccupied.

It is not possible to ensure that computer terminals are always kept out of the reach of unauthorised personnel. However, terminals should never be left unattended when connected to the network, unless they are locked against casual use. Users will be logged out of the network if the computer is idle for 10 minutes or more. All staff are expected to be vigilant with regards to computer access; staff should challenge anyone who appears to be using equipment without permission.

Equal vigilance should be given to paper records. It is acceptable for such records to be kept within private offices, provided the offices are locked, or access restricted, when authorised staff are

absent. Otherwise, personal data held on paper should be kept in locked drawers, cabinets or archive rooms.

Computer passwords

Each authorised user of the Nova computer network is issued with a unique password. Passwords may be changed by request to the Network Administrator. On no account should a personal password be disclosed to any person, other than the Network Administrator or her appointed deputy.

Disclosure of information

On no account should personal data be disclosed to a third party unless staff are absolutely sure that such disclosure is authorised. Disclosure is only permitted if it is within the terms of Nova's Notification under the Data Protection Act. If in doubt, refer the matter to the CEO.

Data storage and sharing information requests from individuals regarding their data should be accommodated. These rights include:

- The **right to be informed** about how their data is used.
- The **right of access** to their personal data (Subject Access Request).
- The **right to rectification** of inaccurate data.
- The **right to erasure** (also known as the "right to be forgotten").
- The **right to object** to the processing of their data, particularly for direct marketing.

Retention of information

Personal data should not be kept for longer than is necessary. Some of the most common type of records that have statutory requirements are listed in the box below:

Record	**Statutory retention period**	**Statutory authority/Reason for retention period**
Accident books, accident records/reports	3 years after the date of the last entry	The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995 (RIDDOR) (SI 1995/3163)
Accounting records	6 – 10 years	Section 221 of the Companies Act 1985/Charities Act

Income tax and NI returns, income tax records and correspondence with the Inland Revenue	not less than 3 years after the end of the financial year to which they relate	The Income Tax (Employments) Regulations 1993 (SI 1993/744)
Records relating to events notifiable under the Retirement Benefits Schemes (Information Powers) Regulations 1995, records concerning decisions to allow retirement due to incapacity, pension accounts and associated documents	6 years from the end of the scheme year in which the event took place, or the date upon which the accounts/reports were signed/completed.	The Retirement Benefits Schemes (Information Powers) Regulations 1995 (SI 1995/3103)
Statutory Maternity Pay records, calculations, certificates (Mat B1s) or other medical evidence	3 years after the end of the tax year in which the maternity period ends	The Statutory Maternity Pay (General) Regulations 1986 (SI 1986/1960)
Statutory Sick Pay records, calculations, certificates, self-certificates	3 years after the end of the tax year to which they relate	The Statutory Sick Pay (General) Regulations 1982 (SI 1982/894)
Wage/salary records (also overtime, bonuses, expenses)	6 years	Taxes Management Act 1970

Personnel Records

Personnel records are kept in a locked filing cabinet in the office. DBS checks, sickness and injury records are held separately.

In accordance with the recommended retention period, Personnel Records are kept for 6 years after employment ceases, to cover the time limit for bringing any civil legal action.

Confidentiality

Nova's Confidentiality policy is set out below.

All paid staff, volunteers and management committee members are expected to abide by this policy. Clients using our services will have the relevant parts of this policy explained to them. All paid staff, volunteers and management committee members will sign the Nova confidentiality agreement during induction.

During your employment or volunteering with Nova you have certain duties:

- Of confidentiality, covering general information about Nova work, processes and procedures and the protection of personal data
- To act in good faith
- To act honestly
- Not to compete with Nova or its services

With the exception of disclosures permitted by the Public Interest Disclosure Act 2023 (amended) you must not disclose any confidential information arising out of your employment or volunteering at any time unless such disclosure is authorised by the Director.

Nova offers the following advice to help you protect sensitive or confidential information:

- Mark documents as confidential and envelopes as “private and confidential”
- Be aware when documents are at risk of exposure e.g., when copying, on view on your desk or PC screen and ensure you log off when moving away from your desk
- When saving a document which contains confidential information, ensure it is saved to the server rather than to the individual computer terminal
- Restrict the circulation of confidential documents
- Be aware of other occupants in ear shot when discussing colleagues, volunteers or service user’s personal information
- When disposing of confidential documents ensure they are shredded and not re-cycled

As a guide, the type of confidential information which you are likely to come into contact with are as follows: financial, funding and business planning, student/client and staff personal matters.

For information on security and monitoring, please see the Nova Use of Email and Electronic Systems Policy in the Staff Handbook.

Breaches of security

If staff are aware of any breach of this policy, or of the security of data generally, they should report this matter to the Director. The CEO must present a report on the incident to the Chair of Trustees within two weeks of notification.

Nova takes allegations of a breach of this policy seriously and will follow the Disciplinary procedure to investigate and deal with such allegations.

The “Soft Opt-in” and Data (Use and Access) Act 2025 (DUAA)

The DUAA has introduced some key changes that are particularly relevant electronic mail marketing (emails, texts, and social media messages).

"Soft Opt-in": The new law may allow your charity to send electronic marketing messages to individuals without their specific consent, as long as certain conditions are met.

Conditions for "Soft Opt-in": To use this new rule, all of the following must apply:

- The communication must be for the purpose of furthering the charity's charitable objectives.

- The individual's contact details were originally collected when they expressed interest in or offered support to the charity.
- The individual was given a clear opportunity to opt-out at the time their details were collected and in every subsequent communication.

Updated: August 2024

Last review date: April 2025

Next review date: March 2026