Data Protection Policy

Document title	Data Protection Policy
Reference number	IGP-02
Version number	Version 5
Date of issue	15/04/2015
Date modified	04/04/2023
Policy owner	Director of Assurance and Compliance
Policy lead(s)	Head of Data Protection
Directorate	Assurance and Compliance

Contents

Introduction

The protection of individuals via the lawful, legitimate and responsible processing and use of their personal data is a fundamental human right. Individuals may have a varying degree of understanding or concern for the protection of their personal data, but the National Autistic Society must respect their right to have control over their personal data and ensure it acts in full compliance with legislative and regulatory requirements at all times. If individuals feel that they can trust our charity is a custodian of their personal data, this will also help our charity to fulfil its wider objectives.

The UK General Data Protection Regulation (UK-GDPR), as supplemented by the Data ProtectionAct DPA 2018 (DPA), is the main piece of legislation that governs how our charity collects and processes personal data. Failure to comply with this legislation may have severe consequences for our charity, including potential fines of up to £17.5 million or 4% of our charity's total annual turnover, whichever is higher.

Summary

This policy sets out how our charity will process the personal data of its staff, volunteers, people we support, research participants, suppliers, supporters and other third parties.

This policy applies to all personal data that our charity processes regardless of the format or media on which the data are stored or who it relates to.

A glossary of the terms used throughout the Policy can be found in Schedule 1.

Scope

This policy applies to all members of staff employed by our charity, including volunteers, contractors and hourly paid staff across all departments, schools and services who must read, understand and comply with this policy when processing personal data in the course of performing their tasks and must observe and comply with all controls, practices, protocols and training to ensure such compliance while carrying out work on behalf of our charity (referredto herein as **you**/**your**) involving the handling personal data.

You have a crucial role to play in ensuring that our charity maintains the trust and confidence of the individuals about whom our charity processes personal data (including its own staff), complying with our charity's legal obligations and protecting our charity's reputation. This Policy therefore sets out what our charity expects from you in this regard.

Compliance with this Policy and the related policies and procedures set out in Schedule 2 is mandatory. Any breach of this Policy and any related policies and procedures may result in disciplinary action.

All members of staff and volunteers across all departments, schools and services must read, understand and comply with this policy when processing personal data in the course of performing their tasks and must observe and comply with all controls, practices, protocols and training to ensure compliance.

The Information Governance Manager/Data Protection Officer is responsible for overseeing the implementation and review of this policy (and the related policies and procedures). They can be contacted as follows:

The National Autistic Society
393 City Road
London
EC1V 1NG

07442 500 872

dataprotection@nas.org.uk

If you do not feel confident in your knowledge or understanding of this policy, or you have concerns regarding the implementation of this policy, it is important that you raise this issue with your line manager as soon as possible or use the contact details above to seek advice.

Roles and responsibilities

Information Governance Manager (Data Protection Officer)
The Information Governance Manager will oversee the information governance framework to ensure that it is operating effectively. This role is also responsible for managing the Society's Information Asset Register and the Society's compliance with the [Data Protection Act/General Data Protection Regulation] and other relevant legislation. This role holds the statutory Data Protection Officer role as designated by the Data Protection Regulation and while they are responsible for overseeing compliance it is the responsibility of the all employees to act upon any recommendations and guidance provided by the DPO in maintaining the confidentiality, integrity and availability of the data. However, where a data privacy impact assessment (DPIA) is required, assistance must be sought from the DPO and IT Director.

Further advice regarding this policy

The Head of Data Protection or other relevant local contacts, can be contacted for general advice and if you:

- wish to process personal data for any purpose and you are unsure whether our charity has a lawful basis for doing so (see Lawfulness and fairness)
- advice and need to prepare a fair processing notice (see Transparency)
- are unsure whether to delete, destroy or keep any personal data (see Storage limitation)
- are unsure about what security or other measures you need to take to protect personal data (see Security, integrity and confidentiality)
- know or suspect that there has been a personal data breach (see Reporting personal data breaches)
- are unsure on what basis to transfer personal data outside of the UK (see Transfers to Third Countries or International Organisations)
- need assistance in dealing with the exercise of any rights by data subjects (see Data subject rights and requests)
- plan to use personal data for any purposes other than those they were originally collected for (see Purpose limitation)
- are considering the processing of personal data in a new or different way, where a Data Protection Impact Assessment may be necessary (see

Accountability and record-keeping)

- plan to undertake any activities involving automated processing including profiling or automated decision-making or any form of biometric processing
- are unsure of the legal requirements relating to any direct marketing activities (see Direct marketing). Additional advice can be sought from our head office marketing team.
- need help with contracts or any other areas in relation to sharing personal data with a third party (see Sharing personal data)

Data Protection Principles

The UK-GDPR is based on a set of core principles that our charity must observe and comply withat all times from the moment that personal data are collected until the moment that personal data are archived, deleted or destroyed.

Our charity must ensure that all personal data are:

1. processed lawfully, fairly and in a transparent manner (Lawfulness, fairness and transparency)
2. collected only for specified, explicit and legitimate purposes (Purpose limitation)
3. adequate, relevant and limited to what is necessary in relation to the purposes for which it is to be processed (Data minimisation)
4. accurate and where necessary kept up to date (Accuracy)
5. not kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed (Storage limitation)
6. processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage (Security, integrity and confidentiality)

Additionally, you must ensure that:

1. Personal data are not transferred outside of the EEA (which includes the use of any website or application that is hosted on servers located outside of EEA) to another country without appropriate safeguards being in place (see Transfers of personal data outside of the EEA)
2. Our charity allows data subjects to exercise their rights in relation to their personal data (see Data subject rights and requests)

Our charity is responsible for, and must be able to demonstrate compliance with all of the above principles (see Accountability and record-keeping).

Lawfulness, fairness and transparency

Lawfulness and fairness

In order to collect and process personal data for any specific purpose, our charity must always have a lawful basis for doing so. Without a lawful basis for processing, such processing will be unlawful and unfair and may also have an adverse impact on the affected data subjects. No data subject should be surprised to learn that their personal data has been collected, consulted, used or otherwise processed by our charity.

Processing personal data will only be lawful where at least one of the following lawful bases applies:

1. The data subject has given their **consent** for one or more specific purposes
2. The processing is necessary for the **performance of a contract** to which the data subject is a party (for instance a contract of employment or registration with our charity)
3. To comply with our charity's **legal obligations**
4. To protect the **vital interests** of the data subject or another person (this will equate to a situation where the processing is necessary to protect the individual's life)
5. To perform tasks carried out in the public interest or the exercise of official authority (generally Care, teaching and research in our charity's case)
6. To pursue our charity's **legitimate interests** where those interests are not outweighed by the interests and rights of data subjects (only available to our charity in some circumstances)

Our charity must identify and document the lawful basis relied upon by it in relation to the processing of personal data for each specific purpose or group of related purposes.

Consent as a lawful basis for processing

There is no hierarchy between the lawful bases for processing above, of which a data subject's consent is only one. Consent may not be the most appropriate lawful basis depending on the circumstances.

In order for a data subject's consent to be valid and provide a lawful basis for processing, it must be:

- **specific** (not given in respect of multiple unrelated purposes)
- **informed** (explained in plain and accessible language)
- **unambiguous** and given by a clear affirmative action (meaning opt-in: silence, inactivity or pre-ticked boxes will not be sufficient)
- **separate and unbundled** from any other terms and conditions provided to the data subject
- **freely and genuinely given** (there must not be any imbalance in the relationship between our charity and the data subject and consent must not be a condition for the provision of any product or service)

A data subject must be able to withdraw their consent as easily as they gave it.

Transparency

The concept of transparency runs throughout the UK-GDPR and requires our charity to ensure that any information provided by our charity to data subjects about how their personal datawill be processed is concise, easily accessible, easy to understand and written in plain language. Where our charity has not been transparent about how it processes personal data, this will call the lawfulness and fairness of the processing into question.

Our charity can demonstrate transparency through providing data subjects with appropriate privacy notices or fair processing notices **before** it collects and processes their personal data and at appropriate times throughout the processing of their personal data.

The UK-GDPR sets out a detailed list of information that must be contained in all privacy noticesand fair processing notices, including the types of personal data collected; the purposes forwhich they will be processed; the lawful basis relied upon for such processing (in the case oflegitimate interests, our charity must explain what those interests are); the period for which they will be retained; who our charity may share the personal data with; and, if

our charity intends to transfer personal data outside of the EEA, the mechanism relied upon for such transfer (see Transfers of personal data outside of the EEA).

Where you obtain any personal data about a data subject from a third party (for example, CVs from recruitment agents for potential employees or DBS checks in relation to our charity's Fitness to Practise Procedures), you must check that it was collected by the third party in accordance with the UK-GDPR's requirements and on a lawful basis where the sharingof the personal data with our charity was clearly explained to the data subject.

All privacy notices and fair processing notices should be reviewed by the Data Protection Officer.

Purpose limitation

You must only collect and process personal data for specified, explicit and legitimate purposes that have been communicated to data subjects **before** the personal data have been collected.

You must ensure that you do not process any personal data obtained for one or more specific purposes for a new purpose that is not compatible with the original purpose. Where you intend to do so, you must inform the data subjects **before** using their personal data for the new purpose and, where the lawful basis relied upon for the original purpose was consent, obtain such consent again.

Data minimisation

The personal data that you collect and process must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is to be processed.

You must only process personal data when necessary for the performance of your duties and tasks and not for any other purposes. Accessing personal data that you are not authorised to access, or that you have no reason to access, may result in disciplinary action and in certain circumstances, may constitute a criminal offence.

You may only collect personal data as required for the performance of your duties and tasks and should not ask a data subject to provide more personal data than is strictly necessary for the intended purposes.

You must ensure that when personal data are no longer needed for the specific purposes for which they were collected, that such personal data are deleted, destroyed or anonymised. You must observe and comply with our charity's Records Management and Retention Policy and Records Retention Schedule.

Accuracy

The personal data that our charity collects and processes must be accurate and, where necessary, kept up-to-date and must be corrected or deleted without delay when our charity discovers, or is notified, that the data are inaccurate.

You must ensure that you update all relevant records if you become aware that any personal data are inaccurate. Where appropriate, any inaccurate or out-of-date records should be deleted or destroyed.

Storage limitation

The personal data that our charity collects and processes must not be kept in a form that identifies a data subject for longer than is necessary in relation to the purposes for which it was collected (except in order to comply with any legal, accounting or reporting requirements).

Storing personal data for longer than necessary may increase the severity of a data breach and may lead to increased costs associated with such storage.

Our charity will maintain policies and procedures to ensure that personal data are deleted, destroyed or anonymised after a reasonable period of time following expiry of the purposes for which they were collected.

You must regularly review any personal data processed by you in the performance of your duties and tasks to assess whether the purposes for which the data were collected have expired. Where appropriate, you must take all reasonable steps to delete or destroy any personal data that our charity no longer requires in accordance with our charity's Records Management Policies.

All privacy notices and fair processing notices must inform data subjects of the period for which their personal data will be stored or how such period will be determined.

You must observe and comply with our charity's Records Management and Retention Policy and Records Retention Schedule.

Security, integrity and confidentiality

Security of personal data

The personal data that our charity collects and processes must be secured by appropriate technical and organisational measures against accidental loss, destruction or damage, and against unauthorised or unlawful processing.

Our charity will develop, implement and maintain appropriate technical and organisational measures for the processing of personal data taking into account the:

- nature, scope, context and purposes for such processing
- volume of personal data processed
- likelihood and severity of the risks of such processing for the rights of data subjects

Our charity will regularly evaluate and test the effectiveness of such measures to ensure that they are adequate and effective.

You are responsible for ensuring the security of the personal data processed by you in the performance of your duties and tasks. You must ensure that you follow all procedures that our charity has put in place to maintain the security of personal data from collection to destruction.

You must ensure that the confidentiality, integrity and availability of personal data are maintained at all times:

- **Confidentiality:** means that only people who need to know and are authorised to process any personal data can access it
- **Integrity:** means that personal data must be accurate and suitable for the intended purposes
- **Availability:** means that those who need to access the personal data for authorised purposes are able to do so

You must ensure that you observe and comply with our Information security policy.

You must not attempt to circumvent any administrative, physical or technical measures our charity has implemented as doing so may result in disciplinary action and in certain circumstances, may constitute a criminal offence.

Reporting personal data breaches

In certain circumstances, the UK-GDPR will require our charity to notify the ICO, and potentiallydata subjects, of any personal data breach.

Our charity has put in place appropriate procedures to deal with any personal data breach and will notify the ICO and/or data subjects where our charity is legally required to do so. If you know or suspect that a personal data breach has occurred, you must contact the Head of Data Protection, and IT Services if relevant, immediately to report it and obtain advice, and take all appropriate steps to preserve evidence relating to the breach.

You must ensure that you observe and comply with our charity's personal data breach procedure.

Sharing personal data

You are not permitted to share personal data with third parties unless our charity has agreed to this in advance, this has been communicated to the data subject in a privacy notice or fair processing notice beforehand and, where such third party is processing the personal data on our behalf, our charity has undertaken appropriate due diligence of such processor and entered into an agreement with the processor that complies with the UK-GDPR's requirements for such agreements.

The transfer of any personal data to an unauthorised third party would constitute a breach of the Lawfulness, fairness and transparency principle and, where caused by a security breach, would constitute a personal data breach. Do not share any personal data with third parties, including the use of freely available online and cloud services for work-related purposes, unless you are certain that the conditions outlined above apply. Seek advice from the Information Governance Manager and Data Protection Officer, or IT Services, if you are unsure.

Transfers to Third Countries or International Organisations

The UK-GDPR makes provisions for the transfer of data to a third country or to an international organisation subject to certain criteria in order to ensure that personal data is not transferred to a country that does not provide the same level of protection for the rights of data subjects. In this context, a "transfer" of personaldata includes transmitting, sending, viewing or accessing personal data in or to a different country.

Our charity may only transfer personal data outside of the EEA if one of the following conditions applies:

- the UK has issued an "adequacy decision" confirming that the country to which we propose transferring the personal data ensures an adequate level of protection for the rights and freedoms of data subjects (this applies to only a small numberof countries)
- appropriate safeguards are in place, such as binding corporate rules, standard contractual clauses that have been approved by the UK, an approved code of conduct or certification mechanism.
- the data subject has given their explicit consent to the proposed transfer, having been fully informed of any potential risks
- the transfer is necessary in order to perform a contract between our charity and a data subject, for reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the data subject in circumstances where the data subject is incapable of giving consent
- the transfer is necessary, in limited circumstances, for our charity's legitimate interests

You must ensure that you do not transfer any personal data outside of the EEA except in the circumstances set out above and provided that our charity has agreed to this in advance.

Data subject rights and requests

The UK-GDPR provides data subjects with a number of rights in relation to their personal data.These include:

- **Right to be informed:** the right to be provided with certain information about how we collect and process the data subject's personal data (see Transparency)
- **Right of subject access:** the right to receive a copy of the personal data that we hold, including certain information about how our charity has processed the data subject's personal data
- **Right to rectification:** the right to have inaccurate personal data corrected or incomplete dated completed
- **Right to erasure (right to be forgotten):** the right to ask our charity to delete or destroy the data subject's personal data if: the personal data are no longer necessary in relation to the purposes for which they were collected; the data subject has withdrawn their consent (where relevant); the data subject has objected to the processing; the processing was unlawful; the personal data have to be deleted to comply with a legal obligation; the personal data were collected from a data subject under the age of 13, and they have reached the age of 13
- **Right to restrict processing:** the right to ask our charity to restrict processing if: the data subject believes the personal data are inaccurate; the processing was unlawful and the data subject prefers restriction of processing over erasure; the personal data are no longer necessary in relation to the purposes for which they were collected but they are required to establish, exercise or defend a legal claim; the data subject has objected to the processing pending confirmation of whether our charity's legitimate interests grounds for

processing override those of the data subject

- **Right to data portability:** in limited circumstances, the right to receive or ask our charity to transfer to a third party, a copy of the data subject's personal data in a structured, commonly-used machine-readable format
- **Right to withdraw consent:** where the lawful basis relied upon by our charity is the data subject's consent, the right to withdraw such consent at any time without having to explain why
- **Right to object:** the right to object to processing where the lawful basis for processing communicated to the data subject was the Society's legitimate interests and the data subject contests those interests
- **Right to object to direct marketing:** the right to request that we do not process the data subject's personal data for direct marketing purposes
- **Right to object to decisions based solely on automated processing (including profiling):** the right to object to decisions creating legal effects or significantlyaffecting the data subject which were made solely by automated means, including profiling, and the right to request human intervention
- **Right to be notified of a personal data breach:** the right to be notified of a personal data breach which is likely to result in a high risk to the data subject's rights or freedoms
- **Right to complain:** the right to make a complaint to the ICO or another appropriate supervisory authority

You must be able to identify when a request has been made and must verify the identity of the individual making a request before complying with it. You should be wary of third parties deceiving you into providing personal data relating to a data subject without their authorisation.

You must immediately forward any request made by a data subject (even if you are uncertain whether it represents a request as set out above) to the Information Governance Manager and Data Protection Officer. Our charity will only have 30 days to respond in most circumstances.

You must observe and comply with our charity data subject access requests procedure.

Research exemption

Some of the rules outlined above do not apply when personal data is being used for research purposes due to an exemption contained in the UK-GDPR and DPA 2018. This exemption applies if the following conditions are met:

a) Appropriate technical and organisational safeguards exist to protect the personal data e.g. data minimisation, pseudonymisation, or access controls.
b) There is no likelihood of substantial damage or distress to the data subjects from the data processing.
c) The research will not lead to measures or decisions being taken about individuals (except for ethically approved interventional medical purposes).
d) Compliance with the requirements that the exemption negates would prevent or seriously impair the research purpose.

If these conditions apply then the following rules can be applied:

a) Personal data originally collected for other purposes can be used for the research and can be kept indefinitely.
b) The right of individuals to access their personal data does not apply if the research results will be made public in a form that does not identify them.
c) The rights of rectification, erasure, restriction and objection do not apply.

Accountability and record-keeping

Our charity is responsible for and must be able to demonstrate compliance with the data protection principles and our charity's other obligations under the UK-GDPR. This is known as the 'accountability principle'.

Our charity must ensure that it has adequate resources, systems and processes in place to demonstrate compliance with our charity's obligations including:

- appointing a suitably qualified and experienced Data Protection Officer (DPO) and providing them with adequate support and resource
- ensuring that at the time of deciding how our charity will process personal data, and throughout its processing, implementing appropriate technical and organisational measures that are designed to ensure compliance with the data protection principles (known as 'Data Protection by Design')
- ensuring that, by default, only personal data that are necessary for each specific purpose are processed both in relation to the nature, extent and volume of such personal data, the period of storage and the accessibility of the personal data (known as 'Data Protection by Default')
- ensuring that where any intended processing presents a high risk to the rights and freedoms of data subjects, our charity has carried out an assessment of those risks and is taking steps to mitigate those risks, by undertaking a '**Data Protection Impact Assessment**' (see below)
- integrating data protection into our charity's internal documents, privacy policies and fair processing notices
- regularly training our charity's staff on the UK-GDPR, this policy and our charity's related policies and procedures, and maintaining a record of training completion by members of staff
- regularly testing the measures implemented by our charity and conducting periodic reviews to assess the adequacy and effectiveness of this policy, and our charity's Related policies and procedures

Our charity must keep full and accurate records of all its processing activities in accordance with the UK-GDPR's requirements.
You must ensure that you have undertaken the necessary training providing by our charity and, where you are responsible for other members of staff, that they have done so.

You must further review all the systems and processes under your control to ensure that they are adequate and effective for the purposes of facilitating compliance with our charity's obligations under this policy.

You must ensure that you observe and comply with all policies and guidance which form our charity's Information Governance Framework.

Data Protection Impact Assessments

A Data Protection Impact Assessment (DPIA), also known as a Privacy Impact Assessment, is a process to help identify and minimise the data protection risks involved in projects, processes and activities involving the processing of personal data. DPIAs are required for processing likely to result in high risk to the individuals and their personal data, and where new technologies are involved. In practice, our charity requires a DPIA for any projects involving the use of personal data, including new systems, solutions and some research studies.

A DPIA must:

- describe the nature, scope, context and purposes of the processing
- assess necessity, proportionality and compliance measures
- identify and assess risks to individuals
- identify any additional measures to mitigate those risks.

DPIAs need to be assessed and signed off by the Data Protection Officer and IT Services.

Our charity's Data Protection Impact Assessment Policy provides full details and a template for conducting a DPIA.

Direct marketing

In addition to our charity's obligations under the UK-GDPR, it is also subject to more specific rulesin relation to direct marketing by email, fax, SMS or telephone.
Our charity must ensure that it has appropriate consent from individuals to send them direct marketing communications, and that when a data subject exercises their right to object to direct marketing it has honoured such requests promptly.

You must ensure that you understand or consult with the DPO on our charity's legal obligations in relation to direct marketing before embarking upon any direct marketing campaign. You must also ensure that you consult the Data Services Team in relation to the use of relevant datasets as they can advise on their proper use in line with the Fundraising Regulators Code of Practice.

Changes to this policy

Our charity may make amendments to this policy at any time without notice, so please ensure you view the latest version.

Appendix 1 : Schedule 1 – Glossary

automated processing	any form of processing (including profiling) that is undertaken by automated means to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning their performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements
consent	any freely given, specific, informed and unambiguous indication of the data subject's wishes by which they, by a statement or by a clear positive action, signifies agreement to the processing of personal data about them
controller	the person or organisation that determines the purposes and means of processing personal data
criminal convictions and offences	personal data relating to criminal convictions, the commission or alleged commission of an offence, proceedings for the commission or alleged commission of an offence and sentencing
Data Protection Impact Assessment (DPIA)	a tool used to identify and reduce the risks of a processing activity and which must be undertaken in certain circumstances specified in the UK-GDPR, also known as 'Privacy Impact Assessments). (See our charity's Data Protection Impact Assessment policy)
data subject	an individual to whom personal data relates and who can be identified or is identifiable from personal data
Data Protection Officer (DPO)	a person required to be appointed in specific circumstances under the UK-GDPR and who must have expert knowledge of data protection law and practice, being the organisation's main representative on data protection matters
DPA 2018	the UK Data Protection Act 2018
EEA	the 28 countries in the European Union and Iceland, Lichtenstein and Norway
explicit consent	a higher standard of consent that requires a very clear and specific statement rather than an action which is suggestive of consent
fair processing notices	a notice setting out information that must be provided to data subjects before collecting personal data from them, including notices aimed at a specific group of individuals or notices that are presented to a data subject on a 'just in-time' basis (also known as 'privacy notice' or 'data protection notice')
UK-GDPR	the UK General Data Protection Regulation (Regulation (EU)2016/679)

personal data	any information identifying a data subject or information relating to a data subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal data includes criminal convictions and offences data, special categories of personal data and pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour
personal data breach	a breach of security lead to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed and which compromises the confidentiality, integrity, availability and/or security of the personal data
privacy notices	see fair processing notices above
process, processes, processing	any activity or set of activities which involves personal data including collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or making available, alignment or combination, restriction, erasure or destruction
pseudonymised, pseudonymisation	replacing information that directly or indirectly identifiesan individual with one or more artificial identifiers (for example, a numerical identifier or other code) or pseudonyms so that the data subject cannot be identified without combining the identifier or pseudonym with other information which has been kept separately and securely. Personal data that have been pseudonymised is still treated as personal data (unlike personal data which has been anonymised)
special categories of personal data	previously known as "sensitive personal data" under the Data Protection Act 2018, this means information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and, for the purposes of this policy personal data relating to criminal offences and convictions.
staff	Our charity's agents, consultants, contractors, employees, representatives, trustees and other representatives, including hourly paid staff and students holding a position of employment

Appendix 2 : Legal Framework

Legal framework

- This policy has due regard to legislation, including, but not limited to the following:
- The General Data Protection Regulation (GDPR)
- The Freedom of Information Act 2000
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The School Standards and Framework Act 1998

This policy will also have regard to the following guidance:

- Information Commissioner's Office (2017) 'Overview of the General Data Protection Regulation (GDPR)'
- Information Commissioner's Office (2017) 'Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now'

This policy will be implemented in conjunction with the following other school policies:

- **Records Management Policy**
- **IT Acceptable Use Policy**
- **Social Media Policy**

Further information on data protection policy, procedures and issues, including specific practical guidance on issues of particular relevance to our staff, can be found on our charity's Intranet.