Data Protection Policy

Article 13: *You have the right to find out things and share what you think with others, by talking, drawing, and writing or in any other way unless it harms or offends other people.*

Article 16: *You have the right to privacy.*

Grange Academy

Belong • Believe • Achieve

Reviewer: Catherine Assink – Head of School
Reviewed: January 2021
Due for review: January 2022

Introduction

Grange Academy is committed to providing outstanding educational opportunities for all our pupils and students. This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with the Data Protection Act 1998, and other related legislation. It will apply to information regardless of the way it is collected, used, recorded, stored and destroyed, and irrespective of whether it is held in paper files or electronically.

All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities by adhering to these guidelines.

Grange Academy will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.

Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.

Statement of intent

Grange Academy collects and uses personal information about pupils/students, staff, parents/carers and other individuals who come into contact with the organisation. This information is gathered in order to enable Grange Academy to provide education and associated functions. In addition, there may be a legal requirement to collect and use information to ensure that Grange Academy complies with its statutory obligations.

Schools and colleges have a duty to be registered as Data Controllers with the Information Commissioner's Office (ICO), detailing the information held and its use. These details are then available on ICO's website. Schools and colleges also have a duty to issue a Fair Processing Notice to all pupils/students/parents/carers: this summarises the information held on pupils/students, why it is held and the other parties to whom it may be passed on.
Data Protection Registration numbers for each Grange Academy setting can be found at the end of this policy.

Grange Academy will do everything within its power to ensure the safety and security of any material of a personal or sensitive nature.

It is the responsibility of all members of the Grange Academy community to take care when handling, using or transferring personal data that it cannot be accessed by anyone who does not:

- have permission to access that data, and/or
- need to have access to that data.

Data breaches can have serious effects on individuals and/or organisations, can bring the organisation into disrepute and may result in disciplinary action, criminal prosecution and fines imposed by the ICO on Grange Academy and the individuals involved.

Particularly, all transfer of data is subject to risk of loss or contamination. Anyone who has access to personal data must know, understand and adhere to this policy, which brings together the legal requirements contained in relevant data protection legislation and relevant regulations and guidance.

Data protection principles

The Data Protection Act 1998 establishes eight enforceable principles that must be adhered to at all times:

- Personal data shall be processed fairly and lawfully.
- Personal data shall be obtained only for one or more specified and lawful purposes.
- Personal data shall be adequate, relevant and not excessive.
- Personal data shall be accurate and where necessary kept up to date.
- Personal data processed for any purpose 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 Data Protection Act 1998.
- Personal data shall be kept secure i.e. protected by an appropriate degree of security.
- Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection.

Grange Academy is committed to maintaining these principles at all times. Therefore the organisation will:

- Inform individuals why the information is being collected when it is collected
- Inform individuals when their information is shared, and why and with whom it was shared
- Check the quality and accuracy of the information it holds
- Ensure that information is not retained for longer than is necessary
- Ensure that when obsolete information is destroyed, it is done so appropriately and securely
- Ensure that clear and robust safeguards are in place to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded
- Share information with others only when it is legally appropriate to do so

- Set out procedures to ensure compliance with the duty to respond to requests for access to personal information (Subject Access Requests)
- Ensure that Grange Academy staff are aware of and understand our policies and procedures

Everyone in the organisation has the responsibility of handling protected or sensitive data in a safe and secure manner.

Governors and Directors are required to comply fully with this policy in the event that they have access to personal data when engaged in their respective roles.

Personal data

Personal information or data is defined as data that relates to a living individual who can be identified from that data, or other information held.

Grange Academy and individuals will have access to a wide range of personal information and data. The data may be held in a digital format or on paper records. Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances. This will include:

- Personal information about members of the Grange Academy community, including pupils/students, members of staff and parents/carers, e.g. names, addresses, contact details, legal guardianship details, health records, disciplinary records etc.
- Curricular/academic data e.g. class lists, pupil/student progress records, reports, references.
- Professional records e.g. employment history, taxation and National Insurance records, appraisal records and references.
- Any other information that might be disclosed by parents/carers or by other agencies working with families or staff members.

Requests from Police or other official bodies for personal information should be made via the form in Appendix 2.

Responsibilities

Everyone in the organisation has the responsibility of handling protected or sensitive data in a safe and secure manner. Local Advisory Board members and Directors are required to comply fully with this policy in the event that they have access to personal data when engaged in their governance role.

Information for parents/carers – Privacy Notice

In order to comply with the fair processing requirements of the DPA, Grange Academy will inform parents and carers of all pupils and students of the data it collects, processes and holds on pupils/students, the purposes for which the data is held and the third parties (e.g. LA, DfE) to whom it may be passed. This privacy notice will be passed to parents/carers through the website of the relevant Grange Academy setting.

Training and awareness

Staff will receive data handling awareness/data protection training and will be made aware of their responsibilities as described in this policy, through:

- Induction training for new staff
- Staff handbook/induction handbook
- Staff meetings/briefings and Inset days

Physical security

Appropriate building security measures are in place, such as alarms, window bars and deadlocks. Only authorised persons are allowed access to personal files. Information will be locked away securely when not in use. Visitors to Grange Academy settings are required to sign in and out, to wear identification badges whilst on Grange Academy property and are accompanied by Grange Academy staff where appropriate.

Grange Academy operates a Clean Desk Policy across all its sites:

- At known extended periods away from their desks, such as a lunch break, staff should place sensitive working papers in locked drawers.
- At the end of the working day staff should tidy their desks and store all papers and other work-related materials/storage devices in a suitable place e.g. locking desk pedestal or filing cabinet.
- Personal or confidential business information must be protected using security features provided, for example secure print on printers.
- Computers must be logged off/locked or protected with a screen locking mechanism controlled by a password when unattended.
- Staff should take care not to leave confidential material on printers or photocopiers.
- All business-related printed matter must be disposed of using confidential waste bins or shredders.

Data storage and access

Grange Academy will ensure that IT systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them.

Access to protected data will be controlled according to the role of the user. Members of staff will not, as a matter of course, be granted access to the whole management information system.

Users will use strong passwords which must be changed regularly. Passwords must be changed immediately if staff suspect their security has been breached. User passwords must never be shared.

Personal data may only be accessed on machines that are securely password protected. Any device that can be used to access data must be locked if left (even for very short periods).
All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.

Personal data can only be stored on Grange Academy equipment (this includes computers and portable storage media). User-owned equipment must not be used for the storage of personal data.

When personal data is stored on any portable computer system, USB stick or other removable media:

- the data must be encrypted and password protected
- the device must be password protected
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device in line with Grange Academy policy once it has been transferred or its use is complete

Grange Academy has clear policies and procedures for the automatic backing up, accessing and restoring of all data held on Grange Academy systems.

Paper-based protected and restricted material must be held in lockable storage.

Grange Academy recognises that under Section 7 of the DPA, data subjects have a number of rights in connection with their personal data, the main one being the right of access.

Procedures are in place to deal with Subject Access Requests i.e. a written request to see all or part of the personal data held by the data controller in connection with the data subject.

Data subjects have the right to:

- know if the data controller holds personal data about them;
- see a description of that data;
- know the purpose for which the data is processed;
- know the sources of that data;
- know to whom the data may be disclosed;
- receive a copy of all the personal data that is held about them.

Under certain circumstances the data subject can also exercise rights in connection with the rectification, blocking, erasure and destruction of data. Where a request includes data about another person, information may be redacted to protect that person's data.

Secure transfer of data and access outside of Grange Academy settings

Grange Academy recognises that personal data may be accessed by users outside of Grange Academy settings, or transferred to local authorities or other agencies. In these circumstances:

- Users may not remove or copy sensitive or restricted or protected personal data from Grange Academy premises without permission and unless the media is encrypted, password protected and transported securely for storage in a secure location.
- Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (e.g. family members) when outside Grange Academy premises.
- When restricted or protected personal data is required by an authorised user from outside the organisation's premises (e.g. by a member of staff to work from their home), they should preferably have secure remote access to the management information system or learning platform.
- If secure remote access is not possible, users must only remove or copy personal or sensitive data from Grange Academy premises if the storage media, portable or mobile device is encrypted and transported securely for storage in a secure location.
- Where files containing personal data need to be sent via email, the file must be password protected and the password conveyed separately to the recipient.
- All portable and mobile devices and storage media used to store and transmit personal information must be protected using approved encryption software.
- Particular care should be taken if data is taken or transferred to another country, particularly outside Europe, and advice should be taken from the local authority (if relevant) in this event.

Disposal of data

Grange Academy will comply with the requirements for the safe destruction of personal data when it is no longer required.

Data held about individuals will not be kept for longer than necessary for the purposes registered. It is the duty of each Head to ensure that obsolete data is properly erased.

The disposal of personal data, in either paper or electronic form, must be conducted in a way that makes reconstruction highly unlikely. Electronic files must be securely overwritten, in accordance with government guidance; other media must be shredded, incinerated or otherwise disintegrated for data.

Audit logging/reporting/incident handling

It is good practice, as recommended in 'Data Handling Procedures in Government' (Cabinet Office, 2008), that the activities of data users in respect of electronically held personal data will be logged and these logs will be monitored by responsible individuals. The audit logs will be kept to provide evidence of accidental or deliberate.

Data security breaches, including e.g. loss of protected data or breaches of an acceptable use policy.

In the event of an information risk incident, the complaints procedure in the Grange Academy Complaints Policy should be followed. This procedure allows for reporting, managing and recovering from information risk incidents by establishing:

- a 'responsible person' for each incident;
- a communications plan, including escalation procedures;

and resulting in:

- a plan of action for rapid resolution; and
- a plan of action of non-recurrence and further awareness raising.

All significant data protection incidents must be reported either to the Principal/CEO or to the Senior Information Risk Officer (SIRO) who will then contact the Information Commissioner's Office based upon the local incident handling policy and communication plan.

Websites and social media

Grange Academy will ensure that no personal information, including images, will be published on Grange Academy websites or social media e.g. official Twitter account, without permission from the individual/s concerned. Pupil/student and staff access to websites and social media groups is monitored by Grange Academy on a regular basis.

Complaints

Complaints will be handled in accordance with Grange Academy Compliments and Complaints Policy. Complaints relating to information handling may be referred to the Information Commissioner (the statutory regulator).

Further information

Information Commissioner's Office
www.ico.gov.uk
0303 123 1113 or 01625 545745
Grange Academy Registration number: Z355178X