Moor House School and College

Data Protection Policy

Version:	5
This Version Dated:	May 2020
Who needs to read this:	All permanent and other Staff, contractors, volunteers, Trustees & Governors
Review cycle:	Bi-Annually
Status:	Draft/Being Reviewed/Approved by Finance and HR Committee /Sent to Governors/Approved by Governors
Lead Manager:	Bursar
Responsible Committee:	Finance and HR Committee (With infringements reported to Trustees)
Next Review Date:	May 2022

Summary

The purpose of this policy is to identify our responsibilities under the General Data Protection Regulations (GDPR), as well as our obligations under our contracts with the Education Funding Agency and under the National Contract with the Local Authorities.

This policy has been written for all staff, volunteers, contractors, Trustees and Governors at Moor House School & College (Moor House), who will receive training/instructions on their responsibilities and sign that they have read and understand this policy.

This policy should be read in conjunction with the CCTV Policy, E-Safety Policy, Acceptable Use of Technology and Networks Policy, Data Retention and Archiving Policy, and Complaints Policy.

Moor House collects and uses both personal data and sensitive personal data about staff, pupils, parents and other individuals who come into contact with the school. This information is gathered in order to enable it to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that Moor House complies with its statutory obligations. The Bursar has a duty to issue a Privacy notice to all pupils and parents summarising the information held on pupils, why it is held, and the other parties to whom the data may be passed.

This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with the GDPR, and other related legislation. It applies to information regardless of the way it is collected, used, recorded, stored and destroyed, and irrespective of the whether it is held in paper files or electronically.

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

The names of students should not be published in any publicly available way without the express permission of a member of Senior Management Team (SMT). This will only be given where permission has been obtained from the parents of that student and, for students aged 13 and over, from the student. Similarly, the names of staff should not be published in any publicly available way, other than to identify their position within Moor House without their permission.

All potential infringements of this policy must be reported to the Bursar and the relevant SMT member or the Principal immediately. They will then decide what action needs to be taken in line with our Disciplinary Policy.

Data Protection Policy Detail

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

Personal data includes the names of staff, pupils and other people, dates of birth, addresses, NI numbers, school marks, medical information, exam results, SEN assessments and staff development reviews.

Sensitive personal data includes information on race and ethnicity, political opinions, religious beliefs, physical or mental health, sexuality and criminal offences. Greater legal restrictions apply to sensitive personal data. The use of sensitive personal data requires explicit consent which must specify the particular types of data and the specific purposes for which the data may be used.

Data Protection Principles

GDPR contains enforceable principles that must be adhered to at all times, which requires personal data to be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) 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;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) 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;

e) 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

f) 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

Procedures and Practices

The Moor House is committed to maintaining the above principles at all times and will:

- Inform individuals why the information is being collected when it is collected
- Inform individuals when their information is shared and with whom it was shared
- Check the quality and accuracy of the information it holds
- Ensure that information is not retained for longer that is necessary – see the Data Retention Policy
- Ensure that when obsolete information is destroyed that 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
    - Personal data and Sensitive Personal data may only be transmitted by encrypted e-mail or special delivery mail to persons who are authorised to receive it (SEN staff in an LA are likely to be authorised to receive such information, but finance staff are unlikely to be authorised). E-mails are not considered to be safe, as they can be hacked. Examples of encrypted e-mail systems are Egress (Surrey, Greenwich, Havering), Voltage (WSCC) and 7Zip.
    - The Data and IT Manager will confirm which Cloud services comply with legislation.
- Set out procedures to ensure compliance with the duty to respond to requests for access to personal information known as Subject Access Requests – see Appendix 1
- Ensure all users are aware of and understand our policies and procedures. All staff handling personal and/or sensitive personal data will receive annual training on Data Protection.

Information Security Policy

Data protection is the responsibility of all members of staff and Governors.

- Staff must not disclose personal or sensitive personal data to third parties without authorisation from the Bursar or a relevant SMT member.
- Personal or sensitive personal data can only be disclosed to authorised persons on a need to know basis and with the consent of the individuals concerned.
- When sending emails, staff should ensure the anonymity of addressees by making use of the BCC (blind carbon copy) functionality when addressing emails.
- Staff must ensure that they do not retain copies of the personal details of another member of staff, a pupil or a pupil's family on their devices. Data of this type can be accessed via SIMS, therefore, paper copies of lists and/or other pupil data should not be taken home.
- Staff must ensure that devices connected to Moor House accounts are kept secure whilst in and out of school and college and report any loss to the Data and IT Manager immediately.
- Staff must not store school material on cloud folders (other than One drive), unencrypted USB sticks or external hard drives.

- All information kept on computers will be password protected. Secure back-ups of the information stored on the computers will be made on a daily basis.
- All personal or sensitive personal data stored in a paper form will be stored securely.
- All personnel involved in any way with the handling of personal and sensitive personal data will be trained on this data protection policy and on security procedures.
- Staff will support student to make a subject access request under Appendix 1.All breaches of security will be investigated. They will be notified to SMT and the Finance and HR Committee. Where significant, they will also be referred to the Information Commissioner and the Charity Commission.
- Virtual Private Network (VPN) remote access to files is provide to staff with the agreement of their SMT member. This allows staff to access and work on their files remotely, while the files remain on the Moor House IT system. These files cannot be transferred to the local system or be printed locally.
- Staff requiring to take files with any student data, personal data and sensitive personal data off site may only do so with the agreement of their SMT member and only providing that it is held in an encrypted device. Access to the encrypted device must be restricted to the staff member. Information containing information relating to students, personal data and sensitive personal data may only be held off-site where it is in a secure place. It should not be:
  - Left in sight in a parked car, always place in the locked boot of the car
  - Left in an accessible place in a hotel bedroom, always place in a safe or other locked area
  - Left at home in an area that is accessible to visitors and family members

Trustees and Governors are given access to their papers, using Home Access Plus. This proves a secure method to access and down load the papers which are confidential but do not contain personal data and sensitive personal data. The Trustees and Governors are responsible for ensuring that the information is held and disposed of confidentially. If required, the Bursar can arrange for information to be disposed of confidentially.

Should it be necessary for a Trustee or Governor to handle personal data or sensitive personal data, then they should adhere to the same requirements as staff requiring to take this information off site.

Publically available media includes websites, Facebooks, Twitter, Prezi, etc

Department heads are responsible for reviewing periodically their own areas to ensure the rules of storage, protection and disposal are being applied. The Bursar will monitor the application of the policy in relation to Moor House's changing data needs usage and report annually on its effectiveness, and make recommendations for improving the policy and its deployment to the Finance and HR Committee.

Archive and back-up security

The data disposal process is set out in the Data Retention and Archiving Policy.

Complaints

Complaints will be dealt with in accordance with the Complaints Policy. Complaints relating to information handling may be referred to the Information Commissioner (the statutory regulator).

Contacts

The Bursar has lead responsibility for Data Protection within Moor House. If you have any enquiries in relation to this policy please contact the Data and IT Manager or the Bursar. The Bursar will also act as the contact point for any subject access requests.

Further advice and information is available from the Information Commissioners Office. The Education advice and resources are at https://ico.org.uk/for-organisations/education/

Agreement to the Data Protection Policy

I confirm that I have read, understood and agree with this Policy

Name	
Signature	
Date	

Appendix 1

SUBJECT ACCESS REQUEST (SAR)

Procedures for responding to Subject Access Requests made under GDPR.

Rights of Access to Information

Under GDPR any individual has the right to make a request to access the personal information held about them. These procedures relate to subject access requests made under GDPR.

Actioning a subject access request

1. Requests for information must be made in writing; which includes email, and be addressed to the Principal or the Bursar. If the initial request does not clearly identify the information required, then further enquiries will be made.
2. The identity of the requestor must be established before the disclosure of any information, and checks should also be carried out regarding proof of relationship to the child. Evidence of identity can be established by requesting production of:
    - Passport
    - Driving license
    - Utility bills with the current address
    - Birth/marriage certificate
    - P45/P60
    - Credit card or mortgage statement

    This list is not exhaustive
3. Any individual has the right of access to information held about them. However with children, this is dependent upon their capacity to understand (normally age 13 or above) and the nature of the request. The Principal should discuss the request with the child and take their views into account when making a decision. A child with competency to understand can refuse consent to the request for their records. Where the child is not deemed to be competent an individual with parental responsibility or guardian shall make the decision on behalf of the child.
4. The school may only make a charge for the provision of information in exceptional circumstances.
5. The response time for subject access requests, once officially received, is 30 days (**not working or school days but calendar days irrespective of school holiday periods).** However the 30 days will not commence until after clarification of information sought.
6. GDPR allows exemptions as to the provision of some information; **therefore all information will be reviewed prior to disclosure.**
7. Third Party information is that which has been provided by another, such as the Police, Local Authority, Health Care professional or another school. Before disclosing third party information consent should normally be obtained. There is still a need to adhere to the 30 day statutory timescale.
8. Any information which may cause serious harm to the physical or mental health or emotional condition of the pupil or another should not be disclosed, nor should information that would reveal that the child is at risk of abuse or information relating to court proceedings.
9. If there are concerns over the disclosure of the information then additional advice should be sought.

10. Where redaction (information blacked out/removed) has taken place than a full copy of the information should be retained in order to establish, if a complaint is made, what was redacted and why.
11. Information disclosed should be clear, thus any codes or technical terms will need to be clarified and explained. If information contained within the disclosure is difficult to read or illegible, then it should be retyped.
12. Moor House must be able to amend, delete or transfer data promptly upon any justified request, or otherwise be prepared to explain why they will not, and provide details of how an individual's personal data was collected and when.
13. Information can be provided at Moor House with a member of staff on hand to help and explain matters if requested, or provided at face to face handover. The views of the applicant should be taken into account when considering the method of delivery. If postal systems have to be used then registered /recorded mail must be used.

Complaints

Complaints about the above procedures should be made to the Chair of Governors/Trustees who will decide whether it is appropriate for the complaint to be dealt with in accordance with the schools complaint procedure. Complaints which are not appropriate to be dealt with through the schools complaint procedure can be dealt with by the Information Commissioner. Contact details of both will be provided with the disclosure information.

Contacts

If you have any queries concerns regarding this policy/procedure then please contact the Bursar. Further advice and information can be obtained from the Information Commissioners Office, www.ico.gov.uk.