GENERAL DATA PROTECTION REGULATION POLICY

GENERAL STATEMENT

The Directors of Abbotsholme School have overall responsibility for ensuring that records are maintained, including security and access arrangements in accordance with educational and all other statutory provisions.

The Directors, Headteacher and Senior Management Team intend to comply with the requirements and principles of the General Data Protection Regulations 2018 which updates the Data Protection Act 1984 and 1998. All staff involved with the collection, processing and disclosure of personal data are aware of their duties and responsibilities within these guidelines.

1 POLICY STATEMENT

1.1 Everyone has rights with regard to how their personal information is handled. During the course of our normal activities, Abbotsholme School will collect, store and process personal information, and we recognise the need to treat it in an appropriate and lawful manner.

1.2 The types of information that we may be required to handle include details of current, past and prospective staff, students, employees, suppliers, customers and others that we communicate with. The information, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the regulations. The regulations impose restrictions on how we may use that information.

1.3 This policy does not form part of any employee's contract of employment and it may be amended at any time. Any breach of this policy will be taken seriously and may result in disciplinary action.

1.4 The school will adopt the following principles when dealing with personal information;

- Be open and honest with individuals regarding their personal information.
- Inform individuals how the school intends to use any personal data collected about them.
- Handle personal data only in ways the individual could reasonable expect.
- Above all, not use personal information in ways that could unjustifiably have a negative impact on them.

2 STATUS OF THE POLICY

2.1 This policy has been approved by the Directors and SMT. It sets out our rules on data protection and the legal conditions that must be satisfied in relation to the obtaining, handling, processing, storage, transportation and destruction of personal information.

2.2 The Designated GDPR Lead is responsible for ensuring compliance with the Act and with this policy. That post is held by Mr Richard Mayfield, e-mail address: richard.mayfield@abbotsholme.co.uk, telephone 01889 590217. Any questions or concerns about the operation of this policy should be referred in the first instance to the Designated GDPR Lead. General information about the regulations can be obtained from the Information Commissioner's Office (www.ico.org.uk).

2.3 If you consider that the policy has not been followed in respect of personal data about yourself or others you should raise the matter with the Designated GDPR Lead.

3 DEFINITION OF DATA PROTECTION TERMS

Data is information which is stored electronically, on a computer, or in certain paper-based filing systems.

Data subjects for the purpose of this policy include all living individuals about whom we hold personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal data.

Personal data means data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual (such as a name, address or date of birth) or it can be an opinion (such as a performance appraisal).

Data controllers are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They have a responsibility to establish practices and policies in line with the Act. We are the data controller of all personal data used in our business. The Data Controllers for Abbotsholme are the SMT.

Data users include employees whose work involves using personal data. Data users have a duty to protect the information they handle by following our data protection and security policies at all times.

Data processors include any person who processes personal data on behalf of a data controller. Employees of data controllers are excluded from this definition but it could include suppliers which handle personal data on our behalf.

Processing is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

Sensitive personal data includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Sensitive personal data can only be processed under strict conditions, and will usually require the express consent of the person concerned.

4 PURPOSE

4.1 The General Data Protection Regulations (GDPR) has two principal purposes:

i) To regulate the use by those (known as data controllers) who obtain, hold and process personal data on living individuals, of personal data; and

ii) To provide certain rights (for example, of accessing personal information) to those living individuals (known as data subjects) whose data is held.

4.2 The cornerstones of the Act are the eight data protection principles, which prescribe:

i) Guidelines on the information life-cycle (creation / acquisition; holding; processing; querying; amending; editing; disclosure or transfer to third parties; and destruction ('the life cycle');

ii) The purpose for which data is gathered and held; and

iii) Enshrine the rights for data subjects.

4.3 The Act applies to the School, the Data Controller for the purposes of the Act, and to anyone who holds personal information in a structured way so that retrieval is easy. The School is fully committed to abiding not only to the letter, but also the spirit of the Act, and, in particular is committed to the observation, wherever possible, of the highest standard mandated by the Act. This policy has been written to acquaint all staff with their duties under the Act and to set out the standards expected by the School in relation to the processing of personal data and safeguarding individuals' rights and freedoms.

5 STAFF DUTIES

Employees of the School are expected to:

i) Acquaint themselves with, and abide by, the Data Protection Principles;

ii) Read and understand this policy document

iii) Understand how to conform to the standard expected at any stage in the life cycle;

iv) Understand how to conform to the standard expected in relation to safeguarding data subject's rights (e.g. the right to inspect personal data) under the regulations;

v) Understand what is meant by 'sensitive personal data', and know how to handle such data;

vi) Contact the Designated GDPR Lead if in any doubt, and not to jeopardise individuals' rights or risk a contravention of the Act.

6 DATA PROTECTION PRINCIPLES

Anyone processing personal data must comply with the eight enforceable principles of good practice. The Data Protection Principles, in summary, are:

i) Personal data shall be processed fairly and lawfully.

ii) Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

iii) Personal data shall be adequate, relevant and not excessive in relation to the purpose(s) for which they are processed.

iv) Personal data shall be accurate and, where necessary, kept up to date.

v) Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or purposes.

vi) Personal data shall be processed in accordance with the rights of data subjects under the Act.

vii) Personal data shall be kept secure. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

viii) 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 protection for the rights and freedoms of data subjects in relation to the processing of personal data.

7 BEST PRACTICE GUIDELINES FOR THE LIFE-CYCLE PROCESS

7.1 Fair and lawful processing (see principles i)

The Act is intended not to prevent the processing of personal data, but to ensure that it is done fairly and reasonably without adversely affecting the rights of the data subject.

For personal data to be processed lawfully, certain conditions have to be met. These may include, among other things, requirements that the data subject has consented to the processing, or that the processing is necessary for the legitimate interest of the data controller or the party to whom the data is disclosed. When sensitive personal data is being processed, more than one condition must be met.

In most cases the data subject's explicit consent to the processing of such data will be required.

7.2 Acquisition of personal data

Those wishing to obtain personal data must comply with guidelines issued from time to time by the Designated GDPR Lead and, in particular, should tell data subjects the purpose(s) for which they are gathering the data, where necessary obtain their specific consent (usually for direct marketing purposes), and inform them (i) that the Schools will be the data controller for the purposes of the Act, (ii) who the data controller's representative is (in this case the Designated GDPR Lead), and (iii) the identities of any other persons to whom the data may be disclosed or transferred.

If sensitive personal data is being collected, explicit consent is not only best practice, it is mandatory. If in doubt individuals must be given the opportunity to 'opt-in' to having their personal data collected and processed, 'opting-out' is not an option.

Personal data should only be collected to the extent that it is required for the specific purpose notified to the data subject. Any data which is not necessary for that purpose should not be collected in the first place.

7.3 Holding / safeguarding / disposal of personal data

Personal data should not be held for longer than is necessary. This means that data should be destroyed or erased from our systems when it is no longer required. Personal records should be reviewed periodically to check that they are accurate and up to date and to determine whether retention is still necessary. For guidance on how long certain data is likely to be kept before being destroyed, contact the Designated GDPR Lead.

Adequate measures should be taken to safeguard data so as to prevent loss, destruction or unauthorised disclosure. The more sensitive the data, the greater the need for measures to be taken.

Personal data must be accurate and kept up to date. Information which is incorrect or misleading is not accurate and steps should therefore be taken to check the accuracy of any personal data at the point of collection and at regular intervals afterwards. Inaccurate or out-of-date data should be destroyed.

7.4 Processing of personal data

Personal data may only be processed for the specific purposes notified to the data subject when the data was first collected or for any other purposes specifically permitted by the Act. This means that personal data must not be collected for one purpose and then used for another. If it becomes necessary to change the purpose for which the data is processed, the data subject must be informed

of the new purpose before any processing occurs and, if the new purpose is very different, the data subject's consent must be obtained.

Disclosures

The School policy is to exercise its discretion under the Act to protect the confidentiality of those whose personal data it holds.

i) Employees of the School may not disclose any information about applicants, pupils or other employees, including information as to whether or not any person is or has been an applicant, pupil or employee of the Schools unless they are clear that they have been given authority by the School to do so. Particular care should be taken in relation to any posting of personal information on the internet.

ii) No employee of the School may provide references to prospective employers or landlords or others without the consent of the individual concerned. It is therefore essential that where the Schools are given as a referee, the subject of the reference should provide the School with the necessary notification and consent.

iii) No employee may disclose personal data to the police or any other public authority in normal course unless that disclosure has been authorised by the Designated GDPR Lead, the exception being for emergencies or Safeguarding cases.

7.5 Transfers

Personal data should not be transferred outside the School, and in particular not to countries outside the EEA.

i) Except with the data subject's consent; or

ii) Unless that country's data protection laws provide an adequate level of protection; or

iii) Adequate safeguards have been put in place in consultation with the Designated GDPR Lead; or:

iv) In consultation with the Designated GDPR Lead, it is established that other exemptions apply.

7.6 Destruction of personal data

Personal data must not be held for longer than necessary; and when such data has been earmarked for destruction, appropriate measures must be taken to ensure that the data cannot be reconstructed and processed by third parties.

7.7 Acceptable Use Policies

All users (including staff, students and others) of the School ICT system, facilities and services shall comply with the relevant ICT Acceptable Use Policy.

8 DATA SECURITY

8.1 We must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. Data subjects may apply to the courts for compensation if they have suffered damage from such a loss.

8.2 The Act requires us to put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data may only be transferred to a third-party data processor if he/she agrees to comply with those procedures and policies, or if he/she puts in place adequate measures himself/herself.

8.3 Maintaining data security means guaranteeing the confidentiality, integrity and availability of the personal data, defined as follows:

i) Confidentiality means that only people who are authorised to use the data can access it.

ii) Integrity means that personal data should be accurate and suitable for the purpose for which it is processed.

iii) Availability means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on our central computer system instead of individual PCs.

8.4 Security procedures include (but are not limited to):

(a) Physical Security: Alarms, CCTV, Cable Locks, Secure lockable desks, cupboards and storage rooms. Entry Controls are also used, and any stranger seen in entry-controlled areas should be reported.

(b) Logical Security: Security software

(c) Procedural Security: Confidentiality agreements are in place and staff are trained in Data Protection obligations. Confidential Waste Disposal is also used. With regards to equipment, data users should ensure that individual monitors do not show confidential information to passers-by and that they log off (or screen lock) their computer when it is left unattended or left on printers.

9 DATA SUBJECTS' RIGHTS

9.1 Data must be processed in line with data subjects' rights. Data subjects have a right to:

i) Access to any personal information held by the school regarding their own data.

ii) Prevent any direct marketing using their own personal data unless express consent is given to do so.

iii) Have inaccurate data amended.

iv) Have information erased when the school has no legitimate reason for storing it.

v) Prevent any automated decision-making and profiling.

vi) Data portability (to take their own personal information and use it for their own purposes).

9.2 The Schools are fully committed to facilitating access by data subjects ('applicants') to their personal data, while bearing in mind the need to protect other individuals' rights of privacy. Gaining access to an individual's own personal data is called a **Data Access Request**.

9.3 All applicants for Data Access Requests will be expected to submit their request in writing to the Designated GDPR Lead. Applicants who are employees of the School and have a school log in and email account may submit their application by e-mail. Applicants who are not members of the school community must submit supporting documentation which establishes that they are the data subject (or where the application is made by a third party on behalf of the data subject, which

establishes the third party's identity, that of the data subject and a form of authority signed by the data subject is produced).

9.4 The fee for a Data Access Request is £10. All Data Access Requests are to be forwarded to the Designated GDPR Lead if they have not been addressed to him directly.

10 PROVIDING INFORMATION OVER THE TELEPHONE

10.1 Any member of staff dealing with telephone enquiries should be careful about disclosing any personal information held by us. In particular they should:

i) Check the caller's identity to make sure that information is only given to a person who is entitled to it.

ii) Suggest that the caller put their request in writing if they are not sure about the caller's identity and where their identity cannot be checked.

iii) Refer to the Designated GDPR Lead for assistance in difficult situations. No-one should be bullied into disclosing personal information.

11 REVIEW

This policy will be reviewed periodically by the School to take account of changes in the law and guidance issued by the Information Commissioner. Recommendations for any amendments should be reported to the Designated GDPR Lead. We will continue to review the effectiveness of this policy to ensure it is achieving its stated objectives.

12 DATA PROTECTION CONTACTS

For general enquiries about the Schools' Data Protection Policy and for formal Data Access Requests under the Act:

The Designated GDPR Lead
Abbotsholme School
Rocester
Staffordshire
ST14 5BS

13 DISCIPLINARY CONSEQUENCES OF THIS POLICY

Unlawful obtaining or disclosure of personal data (including the transfer of personal data outside the EEA in contravention of this policy) or any other breach of the Data Protection Act 1998 by staff or students will be treated seriously by the Schools and may lead to disciplinary action up to and including dismissal or suspension.

Updated - 24.05.2018