DATA PROTECTION POLICY (GDPR)

PRIMARY PERSON RESPONSIBLE FOR IMPLEMENTATION AND MONITORING OF THIS POLICY

JAMES EYTLE, BEVERLEY MELLON (PRINCIPALS)

LAST REVIEW DATE

July 2020

NEXT REVIEW

July 2021

Data Protection Policy

Albemarle College is committed to protecting and respecting the confidentiality of sensitive information relating to staff, pupils and parents.

1. Introduction

a. Albemarle College needs to keep certain information about our employees, pupils and other users to allow us, for example, to monitor performance, achievement, and health and safety.

b. To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To do this, we must comply with the Data Protection principles which are set out in the Data Protection Act 1998.

c. In summary these principles state that personal data shall:

i. Be obtained and processed fairly and lawfully.

ii. Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose.

iii. Be adequate, relevant and not excessive for that purpose.

iv. Be accurate and kept up to date.

v. Not be kept for longer than is necessary for that purpose.

vi. Be processed in accordance with the data subject's rights.

vii. Be kept safe from unauthorised access, accidental loss or destruction.

d. All staff who process or use personal information must ensure that they follow these principles at all times. In order to ensure that this happens, the College has developed this Data Protection Policy. This policy does not form part of the contract of employment for staff, but it is a condition of employment that employees will abide by the rules and policies made by the College from time to time. Any failures to follow the policy can therefore result in disciplinary proceedings.

2. The Data Controller and the Designated Data Controllers

a. Albemarle College, as a body, is the Data Controller under the 1998 Act, and the Principals are therefore ultimately responsible for implementation.

However, the Designated Data Controllers will deal with day to day matters.

b. The School has identified its Designated Data Controllers as:

The College Administrators, The Librarian, the Principals, the Vice Principal, the Director of Studies and the College Support Staff.

c. Any member of staff, parent or other individual who considers that the Policy has not been followed in respect of personal data about himself or herself or their child should raise the matter with the Principal, in the first instance.

3. Responsibilities of Staff

a. All staff are responsible for:

i. Checking that any information that they provide to the College in connection with their employment is accurate and up to date.

ii. Informing the College of any changes to information that they have provided, e.g. change of address, either at the time of appointment or subsequently. The College cannot be held responsible for any errors unless the staff member has informed the College of such changes.

iii. Handling all personal data (eg – pupil attainment data) with reference to this policy.

4. Data Security

a. All staff are responsible for ensuring that:

i. Any personal data that they hold is kept securely.

ii. Personal information is not disclosed either orally or in writing or via Web pages or by any other means, accidentally or otherwise, to any unauthorised third party.

b. Staff should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases.

c. Personal information should:

i. Be kept in a filing cabinet, drawer, or safe in a secure office, or;

ii. If it is computerised, be password protected both on a local hard drive and on a network drive that is regularly backed up; and

iii. If a copy is kept on a usb memory key or other removable storage media, that media must itself be password protected and/or kept in a filing cabinet, drawer, or safe.

5. Rights to Access Information

a. All staff, parents and other users are entitled to:

i. Know what information the College holds and processes about them or their child and why.

ii. Know how to gain access to it.
iii. Know how to keep it up to date.
iv. Know what the College is doing to comply with its obligations under the 1998 Act.
b. The College will, upon request, provide all staff and parents and other relevant users with a statement regarding the personal data held about them. This will state all the types of data the College holds and processes about them, and the reasons for which they are processed.
c. All staff, parents and other users have a right under the 1998 Act to access certain personal data being kept about them or their child either on computer or in certain files. Any person who wishes to exercise this right should make a request in writing and submit it to the Principals. The College will ask to see evidence of your identity, such as your passport or driving license, before disclosure of information.
d. The College may make a charge on each occasion that access is requested in order to meet the costs of providing the details of the information held.
e. The College aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 40 days, as required by the 1998 Act.

6. Retention of Data

a. The School has a duty to retain some staff and pupil personal data for a period of time following their departure from the School, mainly for legal reasons, but also for other purposes such as being able to provide references. Different categories of data will be retained for different periods of time.
7. Monitoring and Evaluation
This is ongoing; where any clarifications or actions are needed the Policy will be amended at its next review.

Photography & Images

Where the capture or distribution of images of children raises a safeguarding concern, the
Designated Safeguarding Lead (DSL) must be contacted immediately. Further details on safeguarding procedures are available in our Safeguarding policy.

Data Protection Act

Photographs and video images of pupils and staff are classed as personal data under the terms of the Data Protection Act 1998. Therefore, using such images for school publicity purposes requires the consent of either the individual concerned or in the case of pupils, their legal guardians. In line with the Data Protection Act, everyone responsible for using data has to follow strict rules called 'data protection principles'. They must make sure the information is:

used fairly and lawfully

used for limited, specifically stated purposes

used in a way that is adequate, relevant and not excessive

accurate

kept for no longer than is absolutely necessary

handled according to people's data protection rights

kept safe and secure

not transferred outside the UK without adequate protection

Photography and image capture in school

Images of children may be captured as part of the educational process. Recordings of pupils for school purposes will only ever be taken using official school equipment or by a designated external professional. Staff must not take or transmit any recording of pupils on any personal device. Staff should also be aware that taking photographs of colleagues using personal devices should only happen with the permission of that member of staff.

Images of pupils or staff must not be displayed on websites, in publications or in a public place without specific consent. The definition of a public place includes areas where visitors to the school have access. Where photographs are taken at an event attended by large crowds, this is regarded as a public area so it is not necessary to get permission of everyone in a crowd shot.

On occasions, commercial video films may be made of children on educational visits and performing in school productions. The school will inform parents where arrangements have been made for a commercial photographer to film such an event. Parents' media permissions must be kept on file (see parental permission form at the end of this document).