IES BRECKLAND

DATA PROTECTION POLICY

Approved by the Governing Body on

Chair of Governors:

November 2014

1. Purpose and Scope

The purpose of this Data Protection Policy is to ensure that IES Breckland and people working in it are aware of their obligations under the Data Protection Act 1998 and comply fully with that Act.

The policy will be communicated to all staff and they will be expected to understand and abide by it.

2. Principles of the Data Protection Act 1998

The school has a duty to comply with the eight principles of the Act, as summarised below.
Personal information* should be:
1) Fairly and lawfully processed;
2) Only obtained for specified purposes and not processed for any other purpose which is incompatible with that;
3) Adequate, relevant and not excessive;
4) Accurate and up-to-date;
5) Not kept for any longer than is necessary;
6) Processed in line with the rights afforded to individuals under the legislation, including the right of subject access;
7) Kept secure;
8) Not transferred to countries outside the European Economic Area (EEA) without adequate protection.

*On occasion the term personal information rather than personal data has been used for ease of understanding. Within this document the meaning of the two is interchangeable.

3. How the school will abide by the Act

The school will comply fully with the DPA. All staff with access to personal data held by the school will abide by the principles of the Act, will comply with this policy and will accept personal responsibility for any personal data that they are handling on behalf of the school.

In particular the school will:

1. Process personal information only where it is strictly necessary for legitimate school purposes.

2. Collect only the minimum personal information required for those purposes. It will not process excessive personal information.

3. Provide clear information to individuals about how their personal information will be used and by whom.

4. Only process relevant and adequate personal information.

5. Process personal information fairly and lawfully.

6. Maintain an inventory of the categories of personal information processed by the school.

7. Keep personal information accurate and, where necessary, up-to-date.

8. Retain personal information only for as long as is necessary for legal or regulatory reasons or legitimate school purposes.

9. Respect individuals' rights in relation to their personal information, including their rights of subject access.

10. Keep all personal information, in whatever format, secure.

11. Only transfer personal information outside the EEA in circumstances where it can be adequately protected.

12. Only apply the exemptions applicable under information legislation.

13. Have a regular review and audit of the way personal information is held, managed and used and ensure methods of handling personal information are regularly assessed and evaluated.

14. Treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information.

15. Have clear procedures for responding to requests for information.

16. Acknowledge, investigate and fully respond to all complaints relating to a request for information according to the corporate complaints process.

4. Responsibility and Accountability for Data Protection

Principal
Has overall responsibility for ensuring that the school:

a) Manages its information and records properly and is compliant with all the relevant legislation.

b) Complies with this policy;

c) Approves procedures where personal information is processed such as: the management and communication of privacy notices; handling of requests from individuals; the collection and handling of personal information; complaints handling; management of personal information security incidents; and outsourcing and off-shoring of personal information processing.

Staff
All staff have an individual responsibility to ensure that they comply fully with the DPA. It is a criminal offence, to knowingly or recklessly obtain or disclose personal data. Staff should not process any personal data unless they are sure that they are authorised to do so. Staff failing to comply with this policy could be subject to action under the school's disciplinary procedure.

Governors
When handling personal information on school business, governors must comply with this policy and be aware of their responsibilities as individuals under the DPA. They should be mindful that it can be a criminal offence to process personal data in a manner which they know that they are not authorised to do. A breach of this policy by a governor is a potential breach of the (governors') Code of Conduct.

5. Data Processing

5.1 Personal Data Held

The school will maintain an inventory of all the categories of personal information that it holds and the reasons for holding that data. Such inventories will be reviewed and updated at least annually and any changes communicated to the Data Protection Officer as soon as they are made so that the school's notification may be kept up-to-date.

5.2 Security of Personal Data

The need to ensure that data is kept securely means that precautions must be taken against physical loss or damage, and that both access and disclosure must be restricted.

All staff are responsible for ensuring that:

- any personal data which they hold is kept securely; and
- personal information is not disclosed either orally, in writing, electronically or otherwise to any unauthorised person.

Personal information should be:

if hard copy:

- not left lying around;
- kept in a locked filing cabinet or in a locked drawer; and
- disposed of as confidential waste.

if electronic:

- be password protected or kept only on portable media which is itself secure in accordance with the school's policy.
- be deleted in accordance with corporate retention periods and evidence of such deletion recorded to provide for necessary audit trails.

Every electronic system that holds personal information has a designated manager who has overall responsible for controlling access to and the information security of that system. At the current time this is the school's Business Manager.

Advice on making personal data secure is provided by the Data Protection Officer.

Any incidents where personal data has been lost or disclosed to unauthorised recipients should be immediately reported to the Principal who will advise what action should be taken to mitigate the damage.

5.3 External Data Processing

All contracts with third-party providers, where the processing of personal data is required, shall include a requirement for the contractor to comply with the requirements of the Data Protection Act 1998.

5.4 Sensitive and High Risk Personal Data
Sensitive personal data is defined in the DPA as information concerning an individual's:

- racial or ethnic origin
- political opinions
- religious beliefs or other beliefs of a similar nature
- trade union membership
- physical or mental health or condition
- sexual life
- criminal convictions or alleged offences

Extra care must be taken when processing sensitive personal data as additional requirements under the DPA must be met to ensure that the processing is legitimate and safe. The advice of the Principal should be sought before any new processing of sensitive personal data commences.

There is also some personal information which is regarded as high risk and therefore a risk assessment should be carried out and additional security precautions should be implemented before processing such information.

High risk personal information includes, but is not limited to:

- personal bank account and other financial information;
- national identifiers, such as national insurance numbers;
- personal information relating to vulnerable adults and children;
- detailed profiles of individuals;
- sensitive negotiations which could adversely affect individuals; and
- large numbers of records containing personal information.

5.5 Medical Records

These are classed as sensitive personal data under the DPA and, therefore, additional care should be taken when processing this information. In particular, before disclosing the

medical records of anyone as part of a Subject Access Request, the advice of the relevant medical practitioner and the Principal must be sought as to whether the information should be released or not.

5.6 Staff Records and the Monitoring of Staff

The school will comply with the ICO's employment practices code in relation to the processing of staff personal information. This Code exemplifies good practice and strikes a balance between the legitimate expectations of workers that personal information about them will be handled properly and the legitimate interests of employers in deciding how best, within the law, to run their own businesses. In particular, staff monitoring should only be carried out in accordance with this code of practice.

5.7 CCTV monitoring

CCTV monitoring must only be carried out in accordance with the ICO's code of practice on CCTV.

5.8 Recording of Telephone Calls

Individuals must be informed at the beginning of any call if the telephone call is being recorded in any format. Currently the school does not record phone calls. Should this happen, the individual must be advised what information is being recorded, the reasons for recording the information, whether the information will be shared with anyone else and, if so, whom it will be shared with and for how long the information will be retained.

5.9 Publication of Personal Data

Personal data should generally only be made public if there is a legal or statutory requirement to do so. On occasion it may be appropriate to publish personal information with the individual's consent. However, in such cases staff must ensure that the consent is fully informed and freely given. Staff must also be aware that it is possible to withdraw consent at any time and, if that happens, publication of the data must cease immediately.

Staff should be aware that publishing personal information on the school's web pages or internet effectively means that the information is published world-wide and outside the EEA. It, therefore, cannot be protected by the DPA or the European Directive on Personal Privacy. Great care should be taken before publishing any personal information (or any information from which individuals could be identified) in this manner and the approval of both the school's Business Manager and the Principal should be obtained before publication.

5.10 Retention and Disposal of Data

It is the responsibility of the individual service areas holding personal information to ensure that the information that they hold is kept accurate and up-to-date and is not held for any longer than is necessary for the purpose for which it was collected. When the data is no

longer required the service area must dispose of the data safely. Usually we keep documentation / staff files for 7 years following leaving the school. Determining retention periods and disposing of data is covered in the Records Management Society, Retention Guidelines for Schools.

6. Access to Data and Disclosure

6.1 Data Subjects Rights

The school will ensure that the rights of people about whom information is held, can be fully exercised under the Act. These include:

- the right to be informed that processing is being undertaken;
- the right of access to one's personal information;
- the right to prevent processing in certain circumstances; and
- the right to correct, rectify, block or erase information which is regarded as wrong information.

6.1.1 Subject Access

If individuals do require to see their personal data, unless special arrangements already exist to allow them access to the data, they should be encouraged to make a request in writing to the Principal. If in doubt, the Principal will take the recommended view that it is better not to release the information as it can always be released at a later date with little harm whereas if released in error it cannot easily be recovered.

6.1.2 Subject Consent

On occasion individuals give consent for the processing of their personal information. Staff must ensure that any consent given for the processing of personal information is fully informed and freely given and that individuals are aware that they may withdraw consent at any time and what the consequences would be if they withdrew their consent. It is advisable not to rely on consent for the processing of personal data if there is another legitimate criterion for processing which could be applied. Before relying on consent, service areas must consider the impact on the service should individuals refuse or withdraw consent. If it is deemed that the consent of individuals is necessary, staff should be aware that, in the case of sensitive personal data, individuals have to give explicit consent to the processing. It is therefore good practice to obtain written consent in such cases and the school will aim to do this.

6.2 External Disclosure Requests

Requests from external organisations or third parties for personal information about individuals should be passed to the Principal. Under no circumstances should any personal information about any individual be passed outside the school without the authority of the Principal. Requesters would have to put any request in writing and send it to the Principal.

6.3 Sharing Information

6.3.1 Within IES Breckland

Before sharing personal information internally it is the responsibility of individual members of staff to ensure that they have the authority to do so and that the recipient is authorised to receive such information. Failure to do so could lead to action under the school's disciplinary procedure (and, in exceptional circumstances, in criminal charges). If there is any doubt individuals should seek the advice of the Principal.

6.3.2 Externally

There are occasional instances where information is shared with partners or outside organisations through agreement. Each agreement, as a minimum, must clearly state the information that will be shared, the purposes for sharing, the basis on which sharing is carried out and the responsibilities for handling and maintaining the personal data.

7. Governance and Review

Responsibility for maintaining and updating this policy belongs to the Principal. This policy will be reviewed at least every two years. It will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments made to the Data Protection Act 1998. Responsibility for monitoring adherence to this policy belongs to the school's Business Manager who should report to the Principal. Governors and the Principal will review the policy.

8. Status of the Policy

This policy has been approved by the governors on the date at the front. All staff are expected to adhere it. Any failure to follow the policy can result in disciplinary proceedings. Staff should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases. Any member of staff who considers that the policy has not been followed should raise the matter with the Principal or the Chair of Governors if it concerns the Principal.