Data Protection Policy

Introduction

The school policy for Data Protection has been written to reflect the legal requirements of the Data Protection Act. It was developed by the Ambleside Primary Policy working group. The policy was ratified by the Governing Body during the Spring Term 2013.

Aims

Through this policy we aim to:

- Meet the school's legal obligations in accordance with the Data Protection Act 1998
- Ensure that all staff are aware and comply with the eight data protection principles
- Meet the legal rights of Individuals
- Ensure that data collected is used fairly and lawfully
- Ensure that personal data is only processed for operational needs or to fulfil legal requirements
- Take the necessary steps to ensure that personal data is up to date and accurate, and details who is responsible for what
- Explain how data protection applies to all our stakeholders
- Clarify professional conduct related to data protection and how staff will be trained

This data protection policy addresses the rights of staff and the wider stakeholder community of Ambleside Primary School.

Legal Obligations of the Data Protection Act

The Data Protection Act is how the UK implements the European Data Protection Directive.

The Data Protection Act 1998 came into force in March 2001. The EU Data Protection Directive (*also known as Directive 95/46/EC*) is a directive adopted by the European Union, designed to protect the privacy and protection of all personal data collected for or about citizens of the EU. It especially relates to the processing, using or exchanging of such data.

The Data Protection Act aims to ensure that anyone who processes personal information complies with the 8 principles. It provides individuals with important rights, including the right to find out what personal information is held about them.

The Data Protection Act 1998 sets out strict rules for dealing with personal information, known within the Act as 'personal data*.'*

Stricter rules apply to sensitive personal data. This can include information which ranges from religious beliefs to physical or mental health.

The Eight Principles of the Data Protection Act

Information must be:

1. Fairly and lawfully processed
2. Processed for specified purposes
3. Adequate, relevant and not excessive
4. Accurate and up-to-date
5. Not kept for longer than is necessary
6. Processed in line with individuals' rights
7. Secure
8. Not transferred outside the European Economic Area without adequate protection

1. Fairly and lawfully processed

"Fairly" – The Data Protection Act says that data must be processed fairly. This means that when consent is sought, it is informed. Individuals must know why the information will be shared and with whom; how the information will be used, and what might happen as a consequence. They are entitled to request to see what is written about them, with a view to correcting it if necessary.

If data has been obtained without consent, the Data Protection Act states that the individual must be informed at the time of doing so, or soon afterwards.

"Lawfully" – This being within the remit of the job as defined by the legislation of Ofsted/ISA or the Benefits Agency etc. Laws may talk explicitly about the need to share information or this may be implicit.

2. Processed for specified purposes

Staff should ensure that the information which is obtained, held, used, or passed on is relevant only to the specific issue for which it was originally obtained.

3. Adequate, relevant and not excessive

The only information shared is the information needed. Typically this is a summary of the relevant information, stating the essence of the concern, its supporting evidence and no more: "I feel this child has additional needs relating to (…) because…."

4. Accurate and up-to-date

Staff responsible must take measures to check and ensure that any personal information held is accurate and up-to-date. At Ambleside Primary School the school business manager is responsible for implementing a periodic system of auditing the personal information held, to ensure that it is accurate.

5. Not kept for longer than is necessary

As in principles 4 and 6, the length of time for which data is held varies. These time spans are detailed within individual policies e.g. the Staff Absence Management Policy. Documents which are no longer necessary are securely disposed of by shredding.

- Pupil Information is kept for the period of their time at Primary until it is passed onto the secondary school.
- General Staffing Information is kept for their employment within the school plus seven years
- Governance minutes are archived electronically
- Financial Records are kept for a period of six years

For a more detailed breakdown of this, please visit the Information & Record Management Society website: www.irms.org.uk

6. Processed in line with individuals' rights

The Data Protection Act gives individuals rights, including the right of access to information held about them. Staff responsible should regularly review to ensure that any incorrect or out of date information is amended.

7. Secure

All staff are expected to follow security protocol when using the internet, email, databases, filing cabinets, diaries, pupil information etc.
Staff must:

- sign out and date when confidential pupil records are removed from the secure filing cabinet.

Staff must not:

- divulge their password to anyone else;
- write down their password in a place where others might find it;
- divulge information which is sensitive to or specific to the organisation to any individuals or agencies outside of the organisation;
- leave their computer unattended while logged on;
- leave note books /diaries unattended which include information on others;
- give keys to a filing cabinet containing sensitive information to any individuals or agencies outside of the organisation.

8. Not transferred outside the European Economic Area without adequate protection

Individuals trust that the information they provide will not be disseminated to parties outside of the organisation.

Legal Rights of Individuals

All individuals have the legal right to access information that is stored about them. Individuals have a right to stop the use or passing on of information if it is done in a way which causes them substantial distress. An individual has the right to claim compensation for damage caused by breaches of the Data Protection Act. An individual can apply for a court order requiring that inaccurate information is corrected.

Rights to access

Individuals have the right to know what information is held about them within the organisation's computer or filing systems. Individuals can submit a written Subject Access Request requesting to see or have a copy of information held about them. Requests should be put in writing to the School Business Manager, head teacher or the Chair of Governors. Upon receipt of the written request, an appropriate member of staff at Ambleside Primary School will ensure that the information is produced within the 40 days stated in the act. (An individual who has trouble putting their request in writing can ask a member of staff for help).

Any information handed over as a result of a written request should be signed for by that individual, with a statement that the information will not be handed over or made available to any third party without the school being notified of this as bound by the Data Protection Act.

School website

The Ambleside Primary school website at amblesideprimaryschool.co.uk shows some of the range of the school's work; is a source of information for parents, and develops links with the wider community. Safety issues associated with a school website have been considered and put into practice.

- Care has been taken to protect the identity of pupils: where a child's image appears, the name should not, and vice versa.
- Parental permission is obtained before using images on the website. This is conducted when a pupil first joins the school, using the school's admission form.
- Members of staff have the option of having their photograph included in the staff gallery.
- Photographs on the website are protected so that they cannot be copied for any purpose

Security measures in place to protect personal information on laptops

When personal information, particularly pertaining to financial or medical matters, is held on a laptop or other portable device, the device should be encrypted. The level of protection provided by encryption is reviewed and updated periodically to ensure that it is sufficient if the device were to be lost or stolen.

Professional Conduct and training of staff

The School Business Manager is the Nominated Officer responsible for data protection compliance and the primary point of contact for all data protection issues. The Nominated Officer has the responsibility to ensure that all required information, copyright information and school licences concerned with data protection are up to date.
Ensuring that staff understand and comply with this policy secures their awareness of good practice in relation to data protection. All staff are reminded of their duty on the first INSET day of each new academic year. Setting the expectation of putting policy into practice also forms part of the induction programme for new members of staff.

All staff with responsibility for personal data receive training. Line Managers and Administrative staff are more extensively trained than the main body of staff, with the expectation that they lead their teams' understanding and compliance with the policy. Line managers are responsible for regularly reviewing data protection procedures and guidelines within their immediate team.

The following expectations apply to all staff:

- To refer to and use this policy to assist with identifying how data subjects' rights can be appropriately exercised
- Always to process the personal information of any individual in accordance with the eight principles of the Act
- To keep personal data securely for appropriate retention periods, as stated in page three of the policy, then shred them or burn.
- To implement the following security measures to protect personal data:
  1. 'Logging off' from a computer if it is left unattended.
  2. Not sharing passwords with other members of staff, friends or family if they can then access the personal information of others
  3. Changing passwords at least once every half term.
  4. Putting an encryption password on confidential files passed as emails as an added security.
  5. Ensuring that confidential records are locked away securely.
  6. Not leaving pupil/personal information in sight for others to see.
  7. Ensuring key pad doors are always shut to prevent access to data by prohibited parties

8. Making clear on email and letter correspondence whether or not the information is confidential to named parties only.
9. Storing sensitive data in secure cabinets, which are locked when unattended. (*Please note that the school's insurance only covers members of staff who comply with this.*)
10. That any internal / external investigations that are deemed as confidential are not discussed outside of the formal meeting with others.

Enforcement of the data protection act

If an individual believes they have been the victim of a breach of the Data Protection Act they can complain to the ICO. The ICO will make a judgement as to whether it is 'likely' or 'unlikely' that the Data Protection Act has been breached. They can be contacted by the following means:

Tel: 0303 123 1113 Fax: 01625 524510
Website: www.ico.gov.uk

By Post: Head office
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire SK9 5AF

Breach of the Data Protection Policy

Breach of this policy will result in disciplinary action of misconduct or gross misconduct, due to the importance of the Data Protection Act.

The ICO has the power to issue monetary penalties either to organisations or individuals for serious breaches of the Data Protection Act which can result in fines of up to £500,000.

What has to be disclosed under the Data Protection Act

The Data Protection Act covers computer records and manual records. Most computer records about a particular person should be easily found and should be disclosed, removing any third party information.

If data controllers are not subject to the Freedom of Information Act 2000 (FOIA), e.g. public authorities, then subject access requests can only apply to manual records which are part of, or intended to be part of, a relevant filing system. The files which form part of the relevant filing system are structured or referenced in such a way that the information about the applicant can be easily located.

In respect to other public servants, such as the police, there is an exemption under the Data Protection Act that can be applied if the police need information to prevent or detect crime, or catch or prosecute a suspect. However, there are limits on the information you can release. Only if staff are satisfied that the information is going to be used for this purpose and that if they did not release the information it would be likely to prejudice (that is, significantly harm) any attempt by the police to prevent a crime or catch a suspect, then you can disclose this information. If any member of staff has doubts about making such a judgement they should consult a member of the leadership team.

Racial Equality & Equal Opportunities Statement

All children have equal access and inclusive rights to the curriculum regardless of their age, gender, race, ethnicity, religion, belief, disability or ability. We plan work that is differentiated for the performance of all groups and individuals. Ambleside Primary School is committed to creating a

positive climate that will enable everyone to work free from racial intimidation and harassment and to achieve their full potential. Policies are available on each of these that expand on this further.

All staff have equal access and inclusive rights to their work regardless of their age, gender, sexual orientation, race, ethnicity, religion, belief, disability or ability. Ambleside Primary School is committed to creating a positive climate that will enable everyone to work free from racial intimidation and harassment and to achieve their full potential. Policies are available on each of these that expand on this further.

Accessibility of policy documents

Parents and carers are welcome to ask for further information about any policy matter. Copies of all current School policies are available for parents and carers to read. A copy of each policy is displayed in the School lobby and all policies can also be consulted online via the School website at www.amblesideprimaryschool.co.uk. The School will try to arrange for the translation or summary of a document when this is requested by a parent or carer whose first language is not English.

Review

This policy will be reviewed in the spring term 2017.

Appendix

Appendix 1 Summary of data protection requirements
Appendix 2 Examples of the eight principles

Appendix1

Summary of data protection requirements

- The Data Protection Act must be complied with, including observance of the eight principles of the Act.
- All staff are expected to be familiar with the school's Data Protection policy and apply it consistently.
- All staff personal details must be kept up to date.
- All staff are expected to observe good practice by:
  - changing their password termly
  - ensuring that when away from their computer, their screen saver is activated and is password-protected.
  - by ensuring the security of all website photos.
  - applying passwords to all confidential files
  - ensuring linked computers to staff are signed for.

All requests for information and subject access requests must be referred to a member of the leadership team.

Appendix 2

Examples of the eight Principles

1. Fairly and lawfully processed
   CRB Checks
   Spending & Budget allocation
   Application forms from pupils to join the school
   Application forms for staff recruitment

2. Processed for specified purposes
   Safer Recruitment Check List
   Meeting the requirements of the Equality Act

3. Adequate, relevant and not excessive
   Staff Appraisal
   Observations
   Pupil Files
   Behaviour Logs
   Minutes of meetings

4. Accurate and up-to-date
   SIMs
   School Budget
   Pupil Records
   Logs of meetings

5. Not kept for longer than is necessary
   Financial Records
   Monitoring and Observation Records
   Individual Pupil and staff records

6. Processed in line with individuals' rights
   Appraisal
   Medical Clearance
   Occupational Health Forms
   CRB

7. Secure
   Pupil and Staff Files
   Passwords changes regularly for electronically stored data
   Periodic audit of all filing cabinets

8. Not transferred outside the European Economic Area without adequate protection
   Information disclosed for Pupil Residential trips

A reminder for schools to maintain data security

We are aware that consultants and companies offer school improvement services to schools and local authorities. When you consider providing RAISEonline access you need to take into account the Data Protection Act (DPA), ensuring that your data are secure at all times and not used inappropriately. As a result of questions to our helpdesk, we are providing a reminder of your responsibilities. We urge you to fully read this news item and review the full terms and conditions.

It is the responsibility of the school's headteacher and those with delegated responsibility to manage access to their school's RAISEonline data to ensure that data security is maintained at all times, and that the users who have been given access by the school have secure systems in place for the processing and storage of the data. Please refer to the full terms and conditions available at https://www.raiseonline.org/TaC.aspx to see your responsibilities with regard to data security. You can also access these at the bottom of the RAISEonline homepage.

We urge schools not to share their own passwords with anyone including third parties. RAISEonline school accounts grant access to pupil sensitive data within the system and by sharing your password with an unauthorised individual you may be in breach of the Data Protection Act.

The RAISEonline terms and conditions state that users should not share personal data contained within RAISEonline unless they are satisfied those individuals need the information to discharge a statutory education function. They must also ensure that identity and other appropriate checks have been made on an individual prior to issuing them with a username and password. Appropriate checks include checking a person's suitability to access pupils' personal data.

Users must ensure that use of protected data, to which users have access, is consistent with the purpose for which the database was set up and that users do not use protected data for any other purpose. Users must ensure that they process protected data securely and the data are not subject to any unauthorised use or disclosure. Users must not include passwords in any automated log-on process.

Schools and local authorities who provide access to other users (including an external party) should ensure a new account is created with appropriate data and information access rights, keeping in mind not all users should access pupil level data, and that the account is immediately deleted once the user no longer requires access.

You can find out more about the levels of access rights in the RAISEonline library within the 'Frequently asked questions' folder. Tutorials on user administration are also available within the library.

If your password has been accidently disclosed to an unauthorised individual, please ensure that you change it immediately by clicking on the 'Change password' link at the top right corner of the RAISEonline screen, which will appear once you have logged into the system.

To ensure your password is secure it must contain the following:

- at least eight characters in total
- at least one numerical character
- at least one lower case letter
- at least one upper case letter
- at least one special character from this list: **@#£$%^&+=**

IMPORTANT: Note that other characters such as * will not be accepted by the system and the system will not allow you to change your password if all of the above requirements are not met.

If you have any queries, please contact us at enquiries@ofsted.gov.uk.