# Alfriston School

# Data Protection Policy

Reviewed: Sept 2015

Approved by FGB: Sept 2015

Next Review: Sept 2017

## Legal obligations

Schools handle and store personal information about pupils, parents or carers, staff, and governors. Under the Data Protection Act 1998, schools are legally obliged to protect this information. Your school must:

- only collect personal information you need for specific purposes
- keep the information secure
- ensure the information is relevant and up to date
- only hold as much information as you need and only for as long as you need it
- let people know what information is held about them and what it is used for
- allow these people to see the information that is held about them
- notify the Information Commissioner's Office that you process personal information.

## Informing parents and carers

We will send all parents and carers a Privacy Notice annually in the autumn. This gives details of how we hold personal information about each pupil and how we intend to use this information.

## What is a Privacy Notice?

Under the Data Protection Act 1998, all schools and early years settings must inform parents and carers that they hold personal data about each pupil. They must also explain how they intend to use the data and provide information about who the data may be forwarded to.

To comply with this, Alfriston School needs to provide a Privacy Notice to the parents or carers of all new and current pupils, and to the pupils themselves if they are 12 years or older.

## Allowing individuals to see their information

Pupils, their parents or carers, staff and governors have the right to see the personal information schools hold about them and to correct the information if it is wrong. Under the Data Protection Act, you can send a subject access request to the school.

## Notifying the Information Commissioner's Office

All schools have to notify the Information Commissioner's Office (ICO) that they handle personal information. Notification is statutory and failure to do so is a criminal offence.

## Pupils' rights

There are two distinct rights of access to the information schools hold about pupils:

- **Right to the educational record**
  Under the Education (Pupil Information) (England) Regulations 2005; a parent or legal guardian has the right to access their child's educational record.
- **Subject access right**
  Under the Data Protection Act 1998, a pupil has a right to see their own information.

In general, pupils aged 12 years or older should be considered mature enough to make a request. The maturity of young people varies, so your school should treat each request on a case-by-case basis. A parent or legal guardian may also make a request on behalf of their child. However, a parent will only be able to see all the information about their child if the child is unable to act on their own behalf or gives their consent for the information to be released to the parent.

**Timescales for dealing with requests**

If a parent makes a request for information that contains, wholly or in part, an educational record, we will respond within 15 school days.

If a parent makes a subject access request just for personal information outside the educational record, we will respond promptly and at most within 40 calendar days.

**Withholding information**

We can withhold information if providing the information:

- is likely to cause harm to the physical or mental health of the pupil or another person
- would reveal a child is at risk of abuse
- would reveal information about adoption or parental orders
- would reveal information about third parties.

**Legal obligations when dealing with confidential information and ICT**

The school makes every effort to ensure that the confidential information in our care is protected. We make every effort to ensure that information and communication technologies (ICT) are used properly and legally.

The following list gives details of some of the relevant legislation.

**Human Rights Act 1998**

Article 8 of the Human Rights Act gives everyone the right to respect for their private and family life, their home and their correspondence. The right to private life includes the right to have personal information, such as official records, photographs, letters, diaries and medical information kept private and confidential.

**Data Protection Act 1998 (DPA)**

The DPA regulates the handling of personal information relating to living individuals. Personal information includes: your

- name
- contact details
- gender
- ethnicity
- religion
- date of birth
- behaviour

- exam results
- medical history
- offending history.

The DPA requires our school to:

- process personal information fairly and lawfully
- only collect personal information we need for specific purposes
- ensure the information is relevant and up to date
- only hold as much information as we need and only for as long as we need it
- keep personal information secure.

The Act also gives people the right to find out what personal information is held about them on computer and most paper records. So it is important that we manage personal information carefully and keep it for the right amount of time. Personal information is kept in locked cabinets in the school office and in password protected parts of SIMS systems only accessible to named users.

**Common law duty of confidence**

The common law duty of confidence requires that confidential information can be disclosed only with the permission of the person who provided it, or the person the information relates to, unless there is an overriding public interest in disclosing the information without permission. All staff are made aware as part of the induction process of the common law duty of confidence.

**Computer Misuse Act 1990**

The Computer Misuse Act details certain illegal activities, including:

- knowingly using another person's username or password without proper authority
- impersonating another person using email, online chat, web or other services
- misusing authorised access
- using, or helping another person to use, someone else's system for criminal activities
- modifying software or files so as to interfere with the system's operation or to prevent access to or destroy data
- deliberately introducing viruses, worms or other malware to cause a system malfunction.

All staff and pupils are required to sign an acceptable use policy agreement before accessing computers.

**Copyright, Designs and Patents Act 1988**

The Copyright, Designs and Patents Act gives the creators of material control over how it is used, whether the material is on paper, film, CD, DVD, websites or databases.

At Alfriston school we ensure that pupils and staff are aware that:

- all software used within the school must be legally licensed
- material on the internet is protected in the same way as material on other media

- unauthorised use, copying or transmission of copyrighted material is a criminal offence.

**Education and Inspections Act 2006**

Sections 90 and 91 of the Education and Inspections Act provide statutory powers to schools for disciplining pupils for inappropriate behaviour or for not following instructions, both on and off school premises. Section 94 provides a defence for confiscation of inappropriate items from pupils as a disciplinary penalty.

This legislation is important when dealing with e-safety issues. For example, it gives schools the power to intervene in instances of cyberbullying and to confiscate mobile phones and other personal devices from pupils if they are being used to harm the well-being and safety of others.

## Alfriston School is committed to:

- Making sure all staff members with access to pupils' personal information have enhanced CRB or DBS clearance.
- Making sure employment contracts state that misuse of confidential information and information and communication technology (ICT) is a disciplinary matter.
- Making sure confidential information is accessible only to people who have a legitimate need to know it.
- Introducing policies for confidentiality, information security, acceptable use and other areas of information governance. Monitoring their implementation regularly.
- Requiring staff to use strong passwords to access electronically held confidential information.
- Encrypting emails if using them to send confidential information.
- Encrypting portable media used to carry confidential information out of school premises.
- Checking email and internet filter settings on a regular basis to ensure that inappropriate sites are filtered as expected.
- Storing and disposing of confidential records securely.
- Putting in place a procedure for reporting, managing and recovering from information security incidents.
- Log and monitor regularly all information security incidents, allowing for any trends to be picked up and preventative measures to be put in place.
- Train staff and pupils to handle confidential information and ICT responsibly and securely.

## Some 'Dos' and 'Don'ts' for staff handling confidential information

Do:

- change your computer password regularly
- lock or log out of your computer when it is not in use
- report breaches of information security immediately to your line manager.

Don't:

- share your computer and database passwords with other people

- allow pupils or other unauthorised people to access confidential paper or electronic records they do not have a right to see
- disclose confidential information you have access to as part of your work to colleagues, friends or acquaintances who do not have a need to know
- discuss information you have access to as part of your work on any social networking site or any unauthorised website
- look up any information relating to your own family, friends or acquaintances unless you are authorised to do so.

## Storage of personal information

Alfriston School has a legal obligation under the Data Protection Act (DPA) 1998 to keep personal information securely, including secure storage, archival and disposal.

The school is committed to:-

- store and retain all important administrative records for the right amount of time as specified in the *school retention schedule*
- arrange records, both paper and electronic, in a logical order to find them easily and strictly control access to confidential information.
- review records regularly against the school retention schedule to identify those that are of historical significance and need transferring to the East Sussex Record Office (ESRO) and those that can be destroyed.
- transfer records that are no longer used on a frequent basis but need to be retained for administrative, legal or financial purposes to the East Sussex Record Centre. Please note that a cost is involved.
- refer to guidance before transferring records to the Record Centre or the ESRO.
- destroy records identified for disposal securely.

## Using the telephone securely

### All staff should

- Confirm the identity of the caller by telephoning back via a main switchboard or a known and trusted number.
- Check the name and contact details of the person requesting confidential information.
- Release information only if you are able to verify that the caller has a legitimate right to it.
- Ensure confidential conversations cannot be overheard by members of the public, pupils or unauthorised staff.
- Ask if it is safe and convenient to provide personal information at the location from which the person is calling. Arrange an alternative location if necessary.
- Ensure the caller cannot overhear when establishing information. Always put the caller on hold and call back when information has been established.
- Store mobile telephones in a secure location. Keep your telephone with you at all times when you take it off the school premises.
- Report any security breach using the school's formal incident reporting procedure.
- Don't leave personal or confidential details with people who are not entitled to the information. Ask for the relevant person to call back.
- Don't leave personal or confidential details on answer-phones. Leave a message for relevant person to call you back.
- Don't use your own mobile phone or landline to contact pupils and parents. Keep your personal telephone numbers private.

You should take special care to protect the confidentiality of papers, files and documents, including those stored electronically, when they are in your keeping.

## Keeping information secure

### All staff should:-

- Ensure confidential information in their care is not seen by other members of their household, visitors or other unauthorised people.
- Use information relating to school business, including personal information about pupils and staff, only for work purposes.
- Use only school-supplied computers and other equipment for storing confidential information related to school business. Don't store confidential school information on your personal equipment unless authorised to do so.
- Ensure all equipment, documents and materials supplied by the school are used solely for school business purposes. They remain the property of the school and members of the household or other unauthorised people must not be allowed to use them.
- Use only their official school email account for sending or receiving emails related to school business. A personal email account or other email accounts must not be used for this purpose.
- Use only encrypted laptops or memory sticks to carry sensitive or confidential information. Never carry such information on unencrypted electronic media.
- Install up-to-date anti-virus software on their personal computer if using it for school business.
- Keep information and equipment locked out of sight during transport. If they are transporting information or equipment by car, lock it in the boot. Do not leave documents and equipment overnight in the car boot.
- Make sure their wireless (WiFi) connection is encrypted.
- Keep confidential school records and equipment locked away when unattended - they must not be accessible to unauthorised people.
- Keep confidential school records at home for as little time as possible. Return them to their normal filing location in the school as soon as possible.
- Dispose of confidential school information only on school premises. Ensure they follow the appropriate policy.
- Return all school information, equipment and software when no longer needed or on termination of employment. School-supplied computers and portable media should be returned to the school office for correct deletion of information, reformatting or destruction.
- Ensure their personal computer hard disk is erased using erasure software before resale or physically destroyed before disposal.
- Report any security breach to the school as soon as possible, using the school's formal incident reporting procedure

## Transferring confidential information

When removing sensitive or confidential information from school premises, use the most secure method available. The method chosen should be based on:

- the amount of data
- the impact on individuals and the school of losing the data
- the level of risk of losing the data
- the urgency of the data transfer.

Electronic transfer is often the quickest way of sending large amounts of confidential data to other agencies. It can also be the safest way of transferring highly sensitive information from school premises if basic precautions, such as encryption, are taken.

## Transferring confidential information securely

- Use an approved secure transfer mechanism to send confidential information to other agencies. You can use AVCO or S2S for sending and receiving confidential files from East Sussex County Council (ESCC) or other schools.
- Use secure email for sending emails with confidential information to County Council email addresses.
- If secure email is not available, encrypt confidential information using encryption software before emailing it to other agencies. Ensure staff use only encrypted laptops or memory sticks if using them for carrying sensitive or confidential information. Never carry such information on unencrypted electronic media.
- Use Royal Mail signed-for delivery (recorded or special delivery) or a trusted courier for posting highly sensitive information.
- Use fax for sending or receiving sensitive or confidential information only if the need is urgent and there is no more secure alternative available.
- Transfer only as much information as is necessary for the purpose.

## Carrying paper records containing confidential information

Before removing paper records from school premises, staff should make sure there is no other more secure option, such as electronic transfer.

- They should never take an original file or document if it is practical to make and carry a copy. They must assess the impact of loss of the original and make a copy if that impact is unacceptable.
- They should take records out of their secure location only for as long as is necessary and transfer them back to their secure location as soon as possible.
- Carry records in a secure briefcase or container.
- Keep the information with them whenever possible and lock it away securely when they cannot. You should never leave the information in plain sight in public places.
- If transporting the information by car, ensure it is locked in the car boot.
- Keep records secure and confidential while at home. Do not allow family members, friends or colleagues to see the contents or the outside folder of the records.