Freedom of information & Data Protection Policy

(including DBS storage)

Devoran School

Approved by:	Governing Body	**Date:**	19th October
Last reviewed on:	19th October		
Next review due by:	September 2019		

To be read in conjunction with;

Data Protection Act 1998
Freedom of information Act 2000
Education Act 1996
Computer Misuse Act 1980
Communications Act 2003
Malicious Communications Act 1988
Regulation of Investigatory Powers Act 2000
Protection of Children Act 1978
Cloud (Educational Apps) Software Services and the Data Protection Act, DfE 2014
The Police Act 1997
Online safety policy
Acceptable use agreement

The Headteacher and Governing Body have overall responsibility for ensuring that records are maintained, including security and access arrangements, in accordance with Education Regulations and all other statutory provisions. The Headteacher and Governors intend to comply fully with the requirements and principles of the Data Protection Act 1984 and the Data Protection Act 1988. All staff involved with the collection, processing and disclosure of personal data are aware of their duties and responsibilities within these guidelines.

Purpose
The purpose of this policy is to ensure compliance of the school with all its obligations as set out in the Data Protection and Freedom of Information legislation.

Data controller
The School is the Data Controller as defined in the Data Protection Act 1998.

Definitions
Personal data is information that relates to an identifiable living individual that is processed as data. Processing means collecting, using, disclosing, retaining, or disposing of information. The data protection principles apply to all information held electronically or in structured files that tells you something about an identifiable living individual. The principles also extend to all information in education records. Examples would be names of staff and pupils, dates of birth, addresses, national insurance numbers, school marks, medical information, exam results, SEN assessments and staff appraisals.

Sensitive personal data is information that relates to race and ethnicity, political opinions, religious beliefs, membership of trade unions, physical or mental health, sexuality and criminal offences. There are greater legal restrictions on processing sensitive personal data than there are on personal data.

Data subject means an individual who is the subject of personal data or the person to whom the information relates.

Parent has the meaning given in the Education Act 1996, and includes any person having parental responsibility or care of a child.

Data Protection principles
The eight core principles of the Data Protection Act are embedded in this policy in the School's commitment that personal data:

- Is processed fairly and lawfully
- Is obtained only for lawful purposes, and is not further used in any manner incompatible with those original purposes
- Is accurate and, where necessary, kept up to date
- Is adequate, relevant and not excessive in relation to the purposes for which it is processed
- Is not kept for longer than is necessary for those purposes
- Is processed in accordance with the rights of data subjects under the Data Protection Act
- Is protected by appropriate technical and organisational measures against unauthorised or unlawful processing and against accidental loss, destruction or damage
- Is not transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection of the personal information.

Fair processing
Devoran School is committed to being clear and transparent about what type of personal information we hold and how it is used.

Why do we collect information?
The School collects information about our pupils and holds this personal data so that we can:

- Support every pupil's learning
- Monitor and report on every pupil's progress
- Provide appropriate pastoral care and other support for every pupil
- Assess how well every pupil is progressing and report that to the parents.

What type of information do we collect? The information will include:

- Personal data such as name and date of birth as well as contact details;
- Educational performance assessments
- Attendance information
- Pastoral information

It will also include sensitive personal data such as:

- Ethnicity
- Special educational needs
- Behavioural incidents
- Medical information that will help us to support every pupil's education and wider welfare needs

We will also hold personal contact information about parents and carers so that we can contact parents and carers routinely or in an emergency

Where CCTV is used by the School this will only be for general security purposes in order to protect the pupils and staff of the school.

Pupil photographs may be included as part of their personal data and this will be treated with the same level of confidentiality as all other personal data. Photographic images of pupils used in publically available media such as web sites, newsletters or the school prospectus will not identify pupils unless parental permission has been given in advance.

Do we share this information with anyone else?
We do not share any of this data with any other organisation without parental permission except where the law requires it. We are required to provide pupil data to central government through the Department for Education (DfE), the Education Funding Agency (EFA) and the Local Authority (LA). Where it is necessary to protect a child, the school will also share data with the Local Authority Children's Social Services and/or the Police.

Can we see the personal data that is held about our child?
All pupils have a right to access their personal information. As our pupils are under the age of 12 years, parents can request a copy of the child's personal information. This must be in writing to the Chair of Governors. The only circumstances under which the information would be withheld would be if there were a child protection risk, specifically:

- The information might cause serious harm to the physical or mental health of the pupil or another individual
- Where disclosure would reveal a child is at risk of abuse
- Information contained in adoption or parental order records
- Information given to a court in proceedings under the Magistrate's Courts (Children and Young Persons) Rules 1992
- Copies of examination scripts

To protect each child's right of confidentiality under law the school reserves the right to check the identity of a person making a request for information on a child's behalf. On completion of an identity check, the information will be collected and provided within 40 calendar days.

Can we see our child's educational record?
All parents are entitled to a copy of their child's educational record. A request must be made in writing to the Chair of Governors. The Educational Record includes curriculum, assessment, pastoral and behavioural information that is stored by the school. Only information that has come from a teacher or employee of the school or an educational professional contracted by the school can be considered to form part of the educational record. The school will respond to the request within 15 Academy days (21 calendar days excluding any public or school holidays).

Information security
The objective of information security is to ensure that the school's information base is protected against identified risks so that it may continue to deliver its services and obligations to the community. It also seeks to ensure that any security incidents have a minimal effect on its business and academic operations.

Responsibilities
The Headteacher and the Chair of Governors have direct responsibility for maintaining the Information Security policy and for ensuring that the staff of the school adheres to it.

General Security
It is important that unauthorised people are not permitted access to school information and that we protect against theft of both equipment and information. This means that we must pay attention to protecting our buildings against unauthorised access.

Staff must:

- Not reveal pin numbers or building entry codes to people that are not authorised or who cannot prove themselves to be employees
- Beware of people following them into the building or through a security door
- If an unidentified person not wearing a form of identification, ask them why they are in the building
- Not position computer screens on reception desks where members of the public could see them
- Office personnel are to lock secure areas when they are not in the office
- Not let anyone remove equipment or records without authorisation
- Ensure visitors and contractors in school buildings always sign in at the main office and the person they are visiting is to be notified. They must be collected from school reception, DBS details should be retained as appropriate by the school office in a single central record.
- All members of staff must sign the Acceptable Use Agreement

Security
Paper documents should always be filed with care in the correct files and placed in the agreed place in the storage facility.

- Records that contain personal data should be locked away when not in use
- Records must be signed out from the secure storage.
- Files should never be left unattended
- Files are the responsibility of the person who has signed it out

Security of Electronic Data
Most data and information is collected, processed, stored, analysed and reported electronically. It is essential that our systems, hardware, software and data files are kept secure from damage and unauthorised access. School staff must:

- Prevent access to unauthorised persons and to those who have not had the relevant training as this could result in loss of information.
- Keep supplier's CDs containing software safe and locked away, clearly labelled in case they need to be re- loaded.
- When a license is bought buy for software, it usually only covers a certain number of devices. It is important that this number is not exceeded, as this will break the terms of the contract.
- Passwords are a critical element of electronic information security. All staff must manage their passwords in a responsible fashion:
- Don't write it down
- Don't share passwords
- Ensure that your password is something that you can remember but not anything obvious (such as password) or anything that people could guess easily such as your name
- You can be held responsible for any malicious acts by anyone to whom you have given your password
- Include numbers as well as letters in the password
- Take care that no-one can see you type in your password
- Change your password every 90 days, or certainly when prompted. Change it if you think that someone may know what it is.

Many database systems, particularly those containing personal data should only allow a level of access appropriate to each staff member. The level may change over time.

Use of E-Mail and Internet
The use of the school's e-mail system and wider Internet use is for the professional work of the school. Reasonable personal use of the system in a member of staff's own time is permitted but professional standards of conduct and compliance with the school's wider policies are a requirement whenever the e-mail or Internet system is being used. The school uses a filtered and monitored broadband service to protect our pupils. Deliberate attempts to access web sites that contain unlawful, pornographic, offensive or gambling content are strictly prohibited. Staff discovering such sites on the system must report this to their line manager immediately.

The Headteacher will ensure that the sites are reported to the broadband provider for filtering.

- To avoid a computer virus arriving over the Internet, do not open any flashing boxes or visit personal websites
- Do not send highly confidential or sensitive personal information via e-mail unless it is encrypted or password protected
- Save important e-mails straight away
- Unimportant e-mails should be deleted
- Do not send information by e-mail, which breaches the Data Protection Act. Do not write anything in an e-mail which could be considered inaccurate or offensive, and cannot be substantiated
- Always log out of your account / lock your computer when you walk away from the computer

Electronic Hardware

- All hardware held within school should be included on the asset register
- When an item is replaced, the register should be updated with the new equipment removed or replaced
- Do not let anyone remove equipment unless they are authorised to do so by a member of the leadership team

Homeworking Guidance
If staff must work outside of the school or at home, all of the 'Information Security' policy principles still apply. However, working outside of the school presents increased risks for securing information.

The following additional requirements apply:

- Do not access confidential information when you are in a public place, such as a train and may be overlooked
- Do not have conversations about personal or confidential information on your mobile phone when in a public place. Ensure that, if urgent, you have your conversation in a separate room or away from other people

If you use a laptop or tablet or smart phone;

- Ensure that it is locked and password protected to prevent unauthorised access
- Make sure that you don't leave your device anywhere it could be stolen. Keep it with you at all times and secure it when you are in the school
- Any portable device that contains personal data must be encrypted.
- Personal data may not be taking off the school's site or put onto a portable device. Taking personal data off-site on a device or media that is not encrypted would be a disciplinary matter.

The Headteacher will maintain a register of:

- Protected data that has been authorised for use on a portable device
- The fixed period of time that the authorisation relates to
- The reason why it is necessary to place it on the device
- The person who is responsible for the security of the device and its data
- The nature of encryption software used on the devise
- Confirmation of the date that the data is removed from the device.

When working on confidential documents at home do not leave them where others may see them. Dispose of documents using a shredder.

If you are using your own computer, ensure that others cannot access documents. When you have completed working on them, transfer them back to the school's system and delete them from your computer. It is forbidden to use a computer owned by you to hold personal data about pupils or staff at the school.

Audit of Data Access
Where possible our software specifications will include the function to audit access to confidential data and attribute access, including breaches of security, to specific users.

Data Backup
The school will arrange that all critical and personal data is backed up to secure on-line storage. If the school is physically damaged critical data backups will allow the school to continue its business at another location with secure data. Data backup should routinely be managed on a rolling daily process to secure off-site areas.

Disposal of information
Paper records should be disposed of with care. If papers contain confidential or sensitive information shred them before disposing of them. Particular care must be taken when selecting papers to be placed in a recycling bin.

Computers and hardware to be disposed of must be completely professionally 'cleaned' before disposal. It is not enough just to delete all the files.

It cannot be assumed that simply deleting a file will prevent it being recovered from electronic media. Electronic memory containing personal information or sensitive personal information must be electronically scrubbed or physically destroyed.
Where a third-party contractor holds personal information on behalf of the school, for example a

payroll provider, the school will seek reassurance from the contractor regarding their data protection policies and procedures.

Subject Access Requests (SAR)
Requests from parents or pupils for access to personal data or educational records will be dealt with as described in the Privacy Notice for Pupils and their Parents and Guardians. School staff may have access to their personal data within 40 calendar days of a request.

The school will maintain a documented record of all requests for personal information with details of who dealt with the request, what information was provided and when, and any outcomes. The record will be used if there is a subsequent complaint in relation to the request.

Sharing personal information
The school only shares personal information with other organisations where there is a legal requirement to do so or the organisation has been contracted by the school to carry out a function of the school.

The school is required, for example, to share information with the Department for Education and the Education Funding Agency. Under certain circumstances they may also be required to share information with Children's Social Services or the police.

Because our pupils are under the age of 12 years, their own right to access their own personal information held by the school will be exercised through their parents or guardians.

The Headteacher will be responsible for authorising the sharing of data with another organisation. The Headteacher, in authorising the sharing of data will take account of:

- Whether it is lawful to share it
- Whether there is adequate security in place to protect the information while it is being transferred and then held by the other organisation
- Include in the Privacy Notice a simple explanation of who the information is being shared with and why.

Authorised Disclosures
The School will, in general, only disclose data about individuals with their consent. However, there are circumstances under which the School's authorised officer may need to disclose data without explicit consent for that occasion. Authorised recipient will be established through internal checks in accordance with DBS and single central record data held, or through known third party introduction (i.e: social services). These circumstances are strictly limited to:

- Pupil data disclosed to authorised recipients related to education and administration necessary for the school to perform its statutory duties and obligations.
- Pupil data disclosed to authorised recipients in respect of their child's health, safety and welfare.
- Pupil data disclosed to parents in respect of their child's progress, achievements, attendance, attitude or general demeanour within or in the vicinity of the school.
- Staff data disclosed to relevant authorities e.g. in respect of payroll and administrative matters.
- Unavoidable disclosures, for example to an engineer during maintenance of the computer system. In such circumstances the engineer would be required to sign a form promising not to disclose the data outside the school. Officers and IT personnel writing on behalf of the LEA are IT liaison/data processing officers, for example in the LEA, are contractually bound not to disclose personal data.
- Only authorised and trained staff are allowed to make external disclosures of personal data. Data used within the school by administrative staff, teachers and welfare officers will only be made available where the person requesting the information is a professional legitimately working within the school who need to know the information in order to do their work. The

school will not disclose anything on pupils records which would be likely to cause serious harm to their physical or mental health or that of anyone else – including anything which suggests that they are, or have been, either the subject of or at risk of child abuse.

- A 'legal disclosure' is the release of personal information from the computer to someone who requires the information to do his or her job within or for the school, provided that the purpose of that information has been registered.
- An 'illegal disclosure' is the release of information to someone who does not need it, or has no right to it, or one which falls outside the school's registered purposes.

Considerations regarding the method of transferring data should include:

- If personal data is sent by e-mail then security will be threatened.
- Ensure that the recipient's arrangements are secure enough before sending the message.
- The data may also need to be password protected or encrypted
- Circular e-mails sent to parents should be sent bcc (blind carbon copy) so that the e-mail addresses are not disclosed to everyone.
- Similar considerations apply to the use of fax machines. Ensure that the recipient will be present to collect a fax when it is sent and that it will not be left unattended on their equipment.
- If confidential personal data is provided by paper copy it is equally important to ensure that it reaches the intended recipient.

Websites
The school website will be used to provide important information for parents and pupils including our Privacy Notice and our Freedom of Information publication scheme.

Where personal information, including images, are placed on the web site the following principles will apply:

- Personal information will not be disclosed (including photos) on a web site without the consent of the pupil, parent, member of staff or Governor as appropriate
- Compliance with regulations regarding cookies and consent for their use
- The website design specifications will take account of the principles of data protection.

CCTV
If the school uses CCTV this will be notified to the Information Commissioners Office along with the purpose of capturing images using CCTV. The school appreciates that images captured on CCTV constitute personal information under the Data Protection Act.

Photographs
The school may use photographs of pupils or staff taken for inclusion in the printed prospectus or other school publications. Parental consent will be requested for the pupils within the school.

Images recorded by parents using their own personal equipment of their child in a school play or activity for their own family use are not covered by data protection law.

All other uses by the school of photographic images are subject to data protection.

Processing by others
The school remains responsible for the protection of data that is processed by another organisations on its behalf. As part of a contract of engagement other organisations that process data on behalf of the school will have to specify how they will ensure compliance with data protection law.

Training
The Headteacher will ensure that all staff are adequately trained to understand their responsibilities in relation to this policy and procedures. Annual training will take place, delivered by a qualified person.

DBS Storage

General principles

As an organisation using the Disclosure and Barring Service (DBS) service to help assess the suitability of applicants for positions of trust, Devoran School complies fully with the DBS Code of Practice regarding the correct handling, use, storage, retention and disposal of certificates and certificate information. It also complies fully with its obligations under the Data Protection Act 1998 and other relevant legislation pertaining to the safe handling, use, storage, retention and disposal of certificate information and has a written policy on these matters, which is available to those who wish to see it on request.

Storage and access

Certificate information is kept securely, in lockable, non-portable, storage containers with access strictly controlled and limited to those who are entitled to see it as part of their duties. Electronic disclosure information is maintained via a secure electronic password protected system. In addition, the information is held on the school's management information system.

Handling

In accordance with section 124 of the Police Act 1997, certificate information is only passed to those who are authorised to receive it in the course of their duties. We maintain a record of all those to whom certificates or certificate information has been revealed and it is a criminal offence to pass this information to anyone who is not entitled to receive it.

Usage

Certificate information is only used for the specific purpose for which it was requested and for which the applicant's full consent has been given.

Retention

Once a recruitment (or other relevant) decision has been made, we do not keep certificate information for any longer than is necessary. This is generally for a period of up to six months, to allow for the consideration and resolution of any disputes or complaints. The school keeps a copy of the DBS evidence checklist for successful candidates. If, in very exceptional circumstances, it is considered necessary to keep certificate information for longer than six months, we will consult the DBS about this and will give full consideration to the Data Protection and Human Rights of the individual before doing so. Throughout this time, the usual conditions regarding the safe storage and strictly controlled access will prevail.

Disposal

Once the retention period has elapsed, we will ensure that any certificate information is immediately destroyed by shredding. The data of destruction is also recorded on the data destruction database. While awaiting destruction, certificate information will not be kept in any insecure receptacle (e.g. waste bin or confidential waste sack).

We will not keep any photocopy or other image of the certificate or any copy or representation of the contents of a certificate. However, notwithstanding the above, we may keep a record of the date of issue of a certificate, the name of the subject, the type of certificate requested, the position for which the certificate was requested, the unique reference number of the certificates and the details of the recruitment decision taken.