Esbjerg International School

Policies for personal data and data protection

Approved by the Board of Trustees 23rd April 2018

Indholdsfortegnelse

1. Preface and introduction

1.1 Preface

Standard and sensitive personal information, consent form, the registered, data handling agreements etc are just some of the words and concepts that we will hear more and increasingly work with in the future.

The reason for this will be found in the EU adopted personal data regulation which will commence 25th May 2018. At Esbjerg International School we wish to comply by these new regulations, and this involves several aspects among other things change of workflow and more use of IT.

At Esbjerg International School we have chosen to create this policy gathering policies re. IT and DATA in one in order to make it more manageable.

We want to show that we cherish safety and personal data protection both in connection with manual storage of sensitive personal information as well as electronically. With this policy we hope to gain the best possible understanding of this 'new' world which we are all obligated to follow and comply with.

It is quite possible that questions will arise in the near future and in that case, please turn to the people in charge of the different departments and they will assist you.

Jesper Hammer
Business Manager

1.2 Introduction

Every single day we handle personal data, and this applies to both staff as well as students.
It is important that we are in control and understand these concepts and handling these appropriately. For this we make use of different IT-systems which in one way or the other store and keep track of all the different data. The IT-systems are necessary to support the many tasks that we face every day incl. the use of personal data.

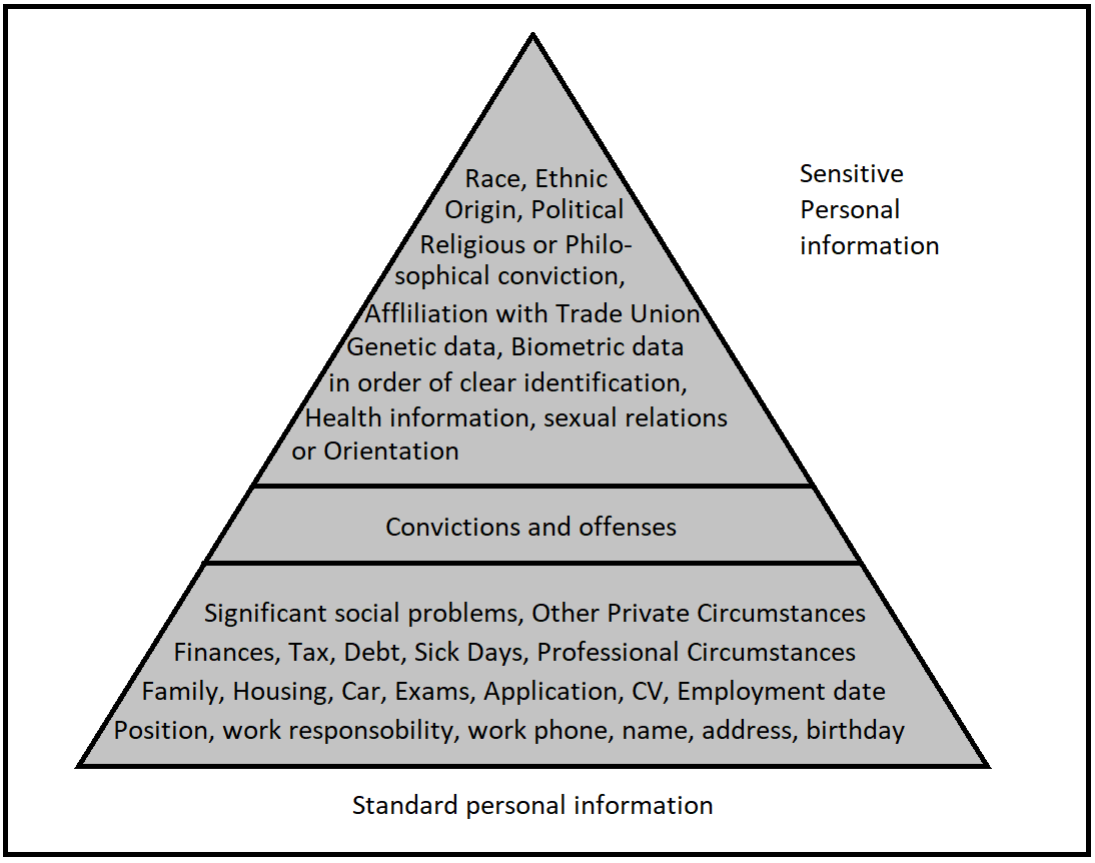
We must establish a framework for the use of IT incl. how we handle data as well as ensuring correct storage and deletion of data. We have created these policies to ensure that we as a school follow the law and the framework that the school has decided on for the use of IT and personal data.

The EU has tightened the requirements for the use of IT and specifically how personal data is handled and the documentation of use. This is what we have considered and worked into the policies.

The policies of Esbjerg International School are split up in the following sections:

- Personal data policy containing a description of how we handle personal data at Esbjerg International School
- Data protection policy at Esbjerg International School
- Use of IT for communication at Esbjerg International School with general rules and practice for how employees and students handle communication and use of IT in daily life

Personal information is any kind of information about an identified or identifiable person.



The above illustration shows examples of what personal information – also referred to as personal data – is, and what the difference between standard personal information and sensitive personal data is. Source: Datatilsynet

2. Personal data policy

2.1 Introduction

This section contains Esbjerg International School's policy for handling personal data for employees, students and visits to the homepage.

2.2 Data responsibility / How do we handle personal data?

We handle personal data as part of the hiring process, in connection with students and visits to the school's homepage.

- Employees
  We handle personal information in the recruiting process, hiring and resignations. Employees can gain insight into the information that will be handled and in which systems the personal data is stored. In connection with resignations there are specific procedures for when the personal data will be deleted.

- Students
  We handle personal data in connection with applications, hiring, tutoring and teaching right up to the point where the student receives their certificate/report card or terminates their education.

- Homepage
  When a user visits our homepage, we register information about this for statistics. We make users aware of this fact when visiting our homepage. When visiting Esbjerg International School's homepage, we always live up to current laws and notices. For further information we refer to the school's cookie policy.

2.3 Disclosure of personal information

Esbjerg International School does not share personal information with third parties. However, there can be statutory laws regulating this. As an example, it can be necessary in connection with changing schools to transfer personal data of a student. There are certain procedures in place for transferring personal data to a third party. If it is not required by law to transfer personal information to a third party, the person in charge of handling the data must obtain consent from the person whom the data is about.

2.4 We take data protection seriously

To protect personal data in the best possible way, we will continue to evaluate possible risks of our data handling having a negative influence on the fundamental rights of the registered.

In the case that the decisions we need to make are depending on us handling sensitive personal data, biometric information or information about criminal offenses, we will analyse the consequences of handling data ensuring protection of privacy.

2.5 Contact information / Data Protection Officer (DPO)

Esbjerg International School is responsible for handling data and ensuring that personal data is handled in compliance with the legislation.

The school have appointed our IT staff to ensure that we live up to rules and procedures for handling data.

For questions on how we handle personal data at Esbjerg International School, please contact:

Haroon Khan (DPO) – IT Manager – E-mail: h.khan@eis.school

Jesper Hammer – Business Manager – E-mail: j.hammer@eis.school

When we in the policies write that "we ask you to make your personal data available for us" it would typically be a specific caseworker handling the case according to the stipulated rules on this.

If you need to send data securely to EIS, you can send it to our secure email:

secure@eis.school

2.6 We ensure fair and transparent data handling

When we request access to personal data, we will inform about the purpose and what data we will be handling. Information will be sent out to the person affected at the time for collecting the personal data.

In general, we would inform about the request for information prior to obtaining it. If not, we will inform no later than 10 days after obtaining the personal data. We will also inform about the purpose and the legal framework allowing us to obtain the personal data.

2.7 We use this type of data

We use data to improve our services and ensure quality in our products and services as well as in our contact with employees, students, parents and externs.

The data that we use include:

2.7.1 We only handle relevant personal data

We only handle data relevant for the purposes defined above. The purpose is defining what type of data is relevant to us. The same applies to the extent of the personal data that we use. We do not use more data than we need for the specific purposes.

Before handling personal data, we examine whether it is possible to minimize the amount of data. We also examine if some of our types of data can be used in an anonymized or pseudonymized form. This we can do if it does not influence our obligations or the services we provide negatively.

2.7.2 We only handle relevant personal data

We only collect, handle and store the personal data necessary to meet our set targets. It can also be determined by law what types of data that are necessary to collect and store to complete our education. The type and the extent of the personal data that we handle can also be necessary in order to live up to a contract or another legal obligation.

We want to ensure that we only handle personal data necessary to each of our set targets. Therefore, we only collect the necessary amount of data.

To protect personal data against unauthorised access we use solutions that automatically safeguards the data and ensures that the data is only accessible to relevant employees. Embedded in these solutions there is also protection against unlimited numbers of people can gain access to the data.

2.7.3 We control and update personal data

We check that the personal data that we handle are not incorrect or misleading. We also keep the personal data up-to-date. As our service is depending on that the data is correct and up-to-date, we ask the registered inform us about relevant changes in data.

To ensure the quality of data, we have agreed on internal rules and settled on procedures for control and updating personal data.

2.7.4 We delete personal data, when they are no longer necessary

We delete personal data, when they are no longer necessary for the purpose which was the reason for collecting, handling and storing the data.

2.7.5 We obtain consent before we handle personal data

We obtain consent before we handle personal data for the purposes described above unless we have a legal basis for obtaining them. We inform about such a basis and about our legitimate interest in handling personal data.

Consent is voluntary and can be withdrawn at any time.

If we wish to use personal data for another purpose than what was originally communicated, we will communicate the new purpose and ask for consent before handling the data. Should there be other legal grounds for handling the data again, we will inform about this.

When we in our education and services need to handle data for re. children under 18, we will obtain consent from a parent. If possible, we will check that consent is given by a parent with custody of the child.

2.7.6 We do not disclose personal data without consent

If we disclose personal data for collaborators for marketing purposes, we obtain consent and communicate what the data will be used for. Objection to this form of disclosure can be made at any time. Marketing purposes can be deselected in the CPR-register.

We do not obtain consent when we are legally obligated to disclose personal data e.g. as part of reporting to an authority.

We obtain consent before we disclose personal data to collaborators in third countries. Should we disclose personal data to collaborators in third countries, we are certain that their level of personal data protection aligns with the requirements established in this policy and in agreement with current legislation. We have demands to how the data is handled, to the information safety and fulfilment of the rights that are in place to e.g. opposing to profiling and filing complaint to Datatilsynet.

2.7.7 We protect personal data and have internal rules for information safety

We have agreed on internal rules re. Information safety; these contain instructions and measures protecting personal data against destruction, to get lost or be altered, against unauthorised publication and against that anyone unauthorised gains access or knowledge about them.

We have set procedures for awarding access rights to those of our employees handling sensitive personal data and data revealing information about personal interests and habits. We check their actual access through logging and inspection. To avoid loss of data we do running backups of our data set. We also protect the confidentiality and the authenticity of data through encryption.

In case of a security breach resulting in a high-level risk of discrimination, ID-theft, economic loss, defamation of character or another significant disadvantage, we will notify the ones affected about the security breach as soon as possible.

If we have an assumption or if we detect a breach of the personal data security, manager must be contacted right away.

2.7.8 Cookies, purpose and relevance

If we place cookies, use and purpose of collecting data via the cookie policy, will be communicated.

Before placing cookies on any equipment, we ask for consent. However, necessary cookies for securing functionality and settings can be used without consent. More information about our ruse of cookies and how they can be deleted or rejected can be found on our homepage. Instructions on withdrawal of consent can be found on our homepage under cookie policy.

2.7.9 Right to access to own personal data

At any time, one has a right to be informed on what data we handle, where they come from and what we use them for. One can also be informed on how long we store the personal data, and who receives data to the extent that we disclose data in Denmark and abroad.

Upon request from the registered, we can inform about the data that we handle. Access can, however, be limited in consideration of other people's protection of privacy, trade secrets and immaterial rights.

Likewise, there is a right to object to how we handle personal data.

2.7.10 Right to have inaccurate personal data corrected or deleted

If the registered believes that the personal data we about the concerned is inaccurate, they have a right to have it corrected.

In some cases, we will have an obligation to delete personal data. This is the case if consent is withdrawn. If the registered find that data is no longer necessary in connection with the purpose for which we obtained consent, the registered can request to have the data deleted. If it is assumed that personal data is handled contrary to the law, it is important to draw attention to this.

When requesting to have personal data corrected or deleted, we will investigate into conditions having been met and, in that case, go through with the corrections or deleting as soon as possible.

2.8 Whistle-blower agreement at Esbjerg International School

Esbjerg International School has not established an actual whistle-blower agreement. We trust that our employees use and handle personal data and it in compliance with the task or assignments they are involved in. Employees sign a confidentiality agreement and as such they are subject to professional secrecy in connection with the different information and personal data that they may come across as part of being an employee at Esbjerg International School. Should an employee suspect any illegalities or irregularities re. personal data or the use of IT, Leadership must be contacted.

3. Data protection policy

3.1 Introduction

This section contains school policy for protection of school data including any personal data we may handle

Data protection is essential for several reasons.

First and foremost, to ensure that Esbjerg International School's sensitive data about students, clients, collaborators and other parts of the organisation does not get passed on to anyone unauthorised.

Secondly to ensure that Esbjerg International School complies with the requirements for the regulations for the protection of personal data including sensitive data re. employees and others.

On this basis Esbjerg International School has provided some rules for protection and handling data in the organisation.

3.2 Contact persons

If in doubt or if there are questions about the data protection policy or about data security, DPO must be contacted – please see contact info under point 2.5

In case of an inadvertent violation of the policy or other breaches of the policy or the security of the data at Esbjerg International Schools data, Leadership must be contacted.

3.3 Use of IT-systems and equipment

Esbjerg International School wish to give employees and students great opportunities for use of IT-systems and equipment without unnecessary restrictions and at the same time secure against abuse of the school's IT-systems and equipment by other systems from the school's installations.

We trust that employees and students exhibit responsibility and common sense when using the school's IT-systems and equipment and that every single user make themselves familiar with the school's general rules and use thereof.

All acquisitions of digital equipment such as pc's, tablets, mobile phones and software must happen through the IT-department via Leadership.

Local application policies with stricter requirements may occur.

Use of IT-facilities:

- Educational and work related use of the school's IT-systems always has preference before private use
- The school's IT-systems and equipment can be used for private purposes under consideration for current policies
- IT-administrators must ensure that IT-systems and equipment is not used for contrary to the purpose. This means that IT-administrators can go through e-mail and other documents. All" 'traffic' is logged. Materials are saved.
- To avoid abuse the user must log off or shut down when the user leaves the equipment
- The network users have an obligation to keep their own password a secret. If a user suspects that others know their password, the user must change their password immediately.
- Exhibit net ethics. This means that the user treats other users on the net with respect. Make sure that own posts can always 'endure' being seen by outsiders
- Avoid unnecessary printing. Be conscious of resources
- When information is handled electronically, only secure and approved IT-systems are used
- Use of private pc, tablet and mobile phone work use must comply with a sworn statement
- If you see materials and behaviours contradicting current policies, Leadership must be contacted.

Examples of inacceptable use of IT-facilities:

- The IT-equipment must not be used for obscene activities or activities against Danish legislation such as laws and regulations re. copyright.
- The user may not change the setting or appearance without an agreement with the one responsible for IT
- It is against the rules to use the IT-systems and equipment for commercial purposes, private marketing, political agitation or publication of private information about another person
- The users must not log on using another person's identity or try to gain access to other users' files or the organisation's files (hacking). The user must not shield their identity except in cases where it is explicitly assigned
- The users may not take part in chain letters or forward an inappropriate number of e-mails in one go (spam)
- It is not legal to install the school's programmes on private pc, tablet or phone without the approval of the IT-department
- One must not save information with sensitive data about others

Consequences by inacceptable use of the IT-facilities:

- Behaviour against the policy of IT-use leads to sanctions and in coarse cases the police
- Sanctions can be verbal as well as written warnings and expulsion

At Esbjerg International School we only use IT-system approved and installed by the IT-department. All purchases and installation of IT-systems are handled by the IT-department. There can be isolated cases or specific conditions leading to that others than the IT-department install IT-systems such as use of systems operated by others.

For further information re. purchase, installation and use of IT-system and equipment, please contact the IT-department.

To support efficiently, the IT-department defines standards for purchases, installation/updating, phasing/renewal, disposal of equipment as well as setting pc work spaces and teaching rooms, printers and more.

3.4 Agreements for handling data

In connection with the personal data agreement it has been agreed that the school should make deals with those IT-suppliers handling personal information on behalf of the school. For this the school uses a standard template developed specifically for this purpose. The school will obtain written consent from the IT-suppliers handling the school's personal information.

The signed agreements will be journalised and filed in the school's filing system. For further information, please contact the IT-department.

Only the IT-department make and approve agreements for handling data.

3.5 E-mails and internet use (social media etc)

All communication, such as e-mails on the school's network is considered school property and must be aligned with the school's guidelines

E-mails and other communication and internet use on the school's equipment and grounds to do with private use must be an exception and must be aligned with the rules about IT-security, behaviour and use of school property.

Use of the school's IT-equipment and property cannot be of pornographic, political extremist or discriminatory nature as far as age, disability, race, gender, ethnic or social origin or religion is concerned.

On resignation – or in cases of redundancy – all references to current employment or links to the organisation must be deleted on social media that the employee can control and/or can make changes in.

Files, belonging to third party, must not be downloaded or in other ways copied or forwarded to the school's equipment and property. Such files can be, but is not restricted to, film clips, photos, games, software programmes and the likes of that. Equivalently, one cannot send materials conflicting with the rules via e-mail.

E-mails and spam from unknown people or companies or organisations must be handled with great care and when in doubt, please contact the IT-department.

E-mails, files or links from unknown sources should never be opened or clicked. This is also the case with e-mails, files or links from known sources if there is any doubt about the authenticity or the security with the sent item.

To the extent that there could be a need to use or handle e-mails or the Internet contrary to the above, it requires approval from the IT-department.

3.6 Passwords

When handling passwords, it is important to pay attention to:

- Passwords needing to be kept in secret and safe.
- Passwords not being shared or passed on to someone else.
- Passwords needing to be changed on a regular basis and at a minimum once a year. Password must, when possible, be at least 8 characters consisting of numbers, letters and symbols.
- Saved passwords cannot be kept by the pc.

3.7 Manual storage of sensitive personal data

Esbjerg International School stores some manual/physical documents with sensitive personal data. An example could be employment contracts, salary slips or registration forms. These are kept safe and are locked in cabinets in offices that are locked when staff with access to this information are not in their offices.

3.8 Disposal of sensitive personal data

Esbjerg International School disposes of sensitive personal data according to the rules. This includes applications, old contracts, student report cards and more. These will be deleted from our systems when the one in question is no longer employed or is a student at school. Physical records will be shredded in a locked container.

3.9 Sanctions

Non-compliance with the data protection policy can, depending on the severity of the violation, lead to a professional reprimand, warning, termination or expulsion.