COPPERFIELD
INTERNATIONAL SCHOOL
VERBIER

Data Protection Policy

Background

Data protection is an important legal compliance issue. The School collects, stores and processes personal data about staff, students, their parents, suppliers and other third parties. The scope of the School's data processing is set out in more detail in its Privacy Statement. It is an area where all staff have a part to play in ensuring we comply with our legal obligations.

This policy sets out the School's expectations and procedures with respect to processing any personal data we collect from data subjects to meet the requirements of the General Data Protection Regulation 2016 (GDPR) and the Data Protection Act 2018 as well as the Swiss Federal Act on Data Protection (FADP) 2020. The Swiss Federal Parliament is responsible for enforcing data protection law and has powers to take action for breaches of the law.
Key data protection terms used in this data protection policy are:

- Data controller – an organisation that determines the purpose and means of processing of personal data. For example, the School is the controller of students' personal information. As a data controller, we are responsible for safeguarding the use of personal data.
- Data processor – an organisation that processes personal data on behalf of a data controller, for example a payroll provider or other supplier of services.
- Personal data breach – a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
- Personal data - any information relating to a living individual (a data subject), including name, identification number, location or online identifier such as an email address. Note that personal information created in the ordinary course of work duties (such as in emails, notes of calls, and minutes of meetings) is still personal data and regulated by data protection laws. Note also that it includes expressions of opinion about the individual or any indication of someone's intentions towards that individual.
- Processing – virtually anything done with personal information, including obtaining or collecting it, structuring it, analysing it, storing it, sharing it internally or with third parties (including making it available to be viewed electronically or otherwise), altering it or deleting it.
- Special categories of personal data – data relating to racial or ethnic origin, political

opinions, religious or philosophical beliefs, trade union membership, health and medical conditions, sex life or sexual orientation, genetic or biometric data used to identify an individual.

Data Protection Leads

The Chief Financial Officer will endeavour to ensure that all personal data is processed in compliance with this policy and data protection law. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to either the Chief Financial Officer.

Data Protection Principles

The GDPR sets out six principles relating to the processing of personal data which must be adhered to by data controllers and data processors. Personal data must be:

1. Processed lawfully, fairly and in a transparent manner;
2. Collected for specific and explicit purposes and only for the purposes it was collected for;
3. Relevant and limited to what is necessary for the purposes it is processed;
4. Accurate and kept up to date;
5. Kept for no longer than is necessary for the purposes for which it is processed; and
6. Processed in a manner that ensures appropriate security of the personal data.

The GDPR's 'accountability' principle also requires that the School not only processes personal data in a fair and legal manner but that we are also able to demonstrate that our processing is lawful. This involves, among other things:

- keeping records of our data processing activities, including logs and policies;
- documenting significant decisions and assessments about how we use personal data.

Lawful grounds for data processing

There are several different lawful grounds for processing personal data. These include 'legitimate interests' and 'performance of a contract'. These two grounds for processing cover a substantial part of the School's processing of personal data. In some circumstances we need the consent of data subjects.

Use of legitimate interests as a ground for processing does require transparency and a

balancing assessment between the rights of the individual and the interests of the Controller, and may be challenged by data subjects.

Other lawful grounds include compliance with a legal obligation, for example in connection with employment, and grounds for processing special categories of personal data (such as health information), which includes explicit consent, emergencies, and specific public interest grounds. Further information on the grounds for processing personal data applied by the School may be found in the School's Privacy Statement.

Summary of Staff Data Protection Responsibilities

Record-keeping

It is vital that the way you record the personal data of others – in particular colleagues, students and their parents – is accurate, professional and appropriate.

The rights of individual data subjects to access data held about them is described in more detail in a later section. This must not discourage staff from recording necessary and sometimes difficult records of incidents or conversations involving colleagues or students, in accordance with the School's other policies, and grounds may sometimes exist to withhold these from such requests. However, the starting position is to record every document or email in such a way that you would be able to stand by it if the person about whom it was recorded were to see it.

It is also important that personal data held by the School about individual members of staff is accurate, fair and adequate. Staff should inform the School if they believe that any personal data relating to them is inaccurate or if they are dissatisfied with the information in any way.

Data handling

All staff have a responsibility to handle the personal data which they come into contact with fairly, lawfully, responsibly and securely and in accordance with the staff handbook and this policy, and all relevant School policies and procedures. In particular, there are data protection implications across a number of areas of the School's wider responsibilities such as safeguarding and IT security, so all staff should, in particular,

read and comply with the following key policies and procedures:

- Safeguarding & Child Protection
- Responsible Use of ICT
- Images protocol
- Social Media

Suppliers/Third Parties

The School also processes data in conjunction with third parties. Where a third party is processing data on the School's behalf, a processing agreement should be in place setting out how the data will be used and the safeguards in place.

If you are sharing information with another organisation which is determining the use of data, as opposed to processing on behalf of the School, it may be the case that a data sharing agreement should be in place. If sharing data we should also be sure of the legal grounds and justification for sharing.

Please contact either the Head of Compliance, Safeguarding and Operations and Chief Financial Officer for advice on the approach to be used.

IT Systems Design and Procurement

The process of designing and implementing new information systems should have data protection considerations at the core of the process. Privacy impact assessment should be carried out and the concept of 'data protection by design'' should be understood and applied.

Avoiding, mitigating and reporting data breaches

Data controllers must report certain types of personal data breach (those which risk an impact to individuals) to the Chief Financial Officer within 72 hours.

In addition, data controllers must notify individuals affected if the breach is likely to result in a "high risk" to their rights and freedoms. In any event, the School must keep a record of any personal data breaches.

If staff are in any doubt as to whether or not you should report something, it is always best to do so. A personal data breach may be serious, or it may be minor, and it may involve fault or not, but the School always needs to know about them to make a decision.

Care and data security

All School staff should be aware of the data protection principles, to attend any training required, and to use their best efforts to comply with those principles whenever they process personal information. Data security is not only an online or digital issue but one that affects daily processes: filing and sending correspondence, notably hard copy documents. Staff should always consider what the most assured and secure means of delivery is, and what the consequences would be of loss or unauthorised access.

We expect all those with management / leadership responsibilities to be particular champions of these principles and to oversee the swift reporting of any concerns and to identify the need for (and implement) regular staff training.

Rights of Individuals

Individual data subjects have a number of rights, including the right of access to their personal data held by a data controller. This is known as the 'subject access right'. Such a request must usually be met within 30 days. If you become aware of a subject access request (or any communication from an individual about their personal data), you must tell the Executive Director as soon as possible.

Individuals also have legal rights to:

- Require us to correct the personal data we hold about them if it is inaccurate;
- Request that we erase their personal data (in certain circumstances);
- Request that we restrict our data processing activities (in certain circumstances);
- Receive from us the personal data we hold about them for the purpose of transmitting it in a commonly used format to another data controller (in certain circumstances);
- Object, on grounds relating to their particular situation, to any of our particular processing activities where the individual feels this has a disproportionate impact on them; and
- Object to automated individual decision-making, including profiling (where a

significant decision is made about the individual without human intervention), and to direct marketing, or to withdraw their consent where we are relying on it for processing their personal data.

Data Security: online and digital

The School must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. In particular care must be taken to ensure compliance with School policy on passwords, and ensuring that if mobile devices or storage are used, these are encrypted.

Data Security: printed information

Care should be taken to dispose of printed information either by shredding or by handing in to the Chief Financial Officer who will ensure that printed information is disposed of correctly.

Processing of Credit Card Data

Staff who are required to process credit card data must ensure that they are aware of and comply with best practice. If you are unsure in this regard please seek further guidance from the Head of Compliance, Safeguarding and Operations and Chief Financial Officer.

Summary

It is in everyone's interests to get data protection right and to think carefully about data protection issues: this means handling all personal information with which you come into contact fairly, lawfully, securely and responsibly.

A good rule of thumb here is to ask yourself questions such as:

- Would I be happy if my own personal information were being used (for example, shared with a third party) in the way I am proposing? Would I expect it?
- Would I wish to stand by how I have recorded this information in an email or official record if the person concerned was able to see it?
- What would be the consequences of my losing or misdirecting this personal data?