Data

Protection

Policy

Contents

Policy Statement

Eaton House Schools are committed to safe, fair and lawful data protection practices in line with the Data Protection Act (DPA) 2018 and The Data Protection, Privacy and Electronic Communications (Amendments, etc) (EU exit) Regulations 2020

This policy applies to all personal data, in all formats.

Eaton House Schools collects and processes data relating to employees, pupils, parents, visitors, governors and contractors and is committed to safeguarding the individuals' privacy and protecting the personal data collected. It sets out principles which should be followed by all who process any personal data/special category personal data and should be read in conjunction with our privacy notice and other associated guidance and policies.

Definitions

Data Controller	A person or organisation that determines the purposes and the means of processing personal data.
Data Processor	An organisation that processes personal data on behalf of the data controller where personal data is shared but no authorisation is given to make any decisions on how the data can be used. e.g. payroll, IT service desk
Data Subject	The identified individual whose personal data is held or processed.
Personal Data	Any information relating to an identified, or identifiable living individual. E.g. name, identification number, IP address, photos, etc
Special Categories of Personal Data	Personal data which is more sensitive and so needs more protection. E.g. racial or ethnic origin, political opinions, religious beliefs, trade union membership, health, sexual orientation, etc
Processing	Anything done to personal data, such as: collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, erasing, destroying, sharing it internally or with third parties
Personal Data Breach	A breach of security leading to accidental or unlawful destruction, loss, alternation, unauthorised disclosure of or access to personal data.

Principles of Data Protection

Data controllers and data processors from Eaton House Schools must adhere to the principles of UK data protection.

1. Data must be processed lawfully, fairly and in a transparent manner in relation to individuals and not further processed in a manner that is incompatible with those purposes
2. Data must be collected for specified, explicit and legitimate purposes
3. Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
4. Data must be accurate and, where necessary, kept up to date.
5. Data must be kept for no longer than is necessary
6. Data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
7. Eaton House Schools must demonstrate accountability by proving that they adhere to data protection law.

These principles must be followed at all times when processing or using personal information. Through appropriate management and strict application of criteria and controls, Eaton House Schools will;

- Observe the conditions regarding the fair collection and use of information including the giving of consent
- Meet its legal obligations to specify the purposes for which information is used
- Collect and process appropriate information only to the extent that it is needed to fulfil our operational needs or to comply with any legal requirements
- Ensure information is kept up to date
- Ensure that information is held for no longer than is necessary
- Ensure that the rights of individuals whom information is held can be fully exercised under GDPR (right to be informed that processing is being undertaken, to access one's personal information, to prevent processing in certain circumstances, and to correct, rectify or erase information that is regarded as incorrect). Please note the school must also abide to the law relevant to safeguarding, employment and health and safety
- Take appropriate technical and organisational security measures to safeguard personal information

- Abide by individuals' right to appeal or complain to the supervisory authority (the Information Commissioner's Office (ICO)) in the event that agreement cannot be reached in a dispute regarding data protection

- Ensure that personal information is not transferred abroad without suitable safeguards as recommended by legislation.

Roles and Responsibilities

This policy applies to all staff employed by Eaton House Schools and to external organisations or individuals working on our behalf.

Governors

The governing board has overall responsibility for ensuring that Eaton House Schools comply with relevant data protection obligations.

Data Protection Officer (DPO)

The Data Protection Officer is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law and developing related policies and guidelines where applicable.

The DPO is the first point of contact for individuals whose data the school processes and for the Information Commissioners Office (ICO).

Eaton House Schools' DPO is the Bursar.

All Staff

All staff are responsible for;

- Checking that any information that they provide to Eaton House Schools in connection with their employment is accurate and up to date.

- Informing Eaton House Schools of any changes to information that they have provided, e.g. change of address, either at the time of appointment or subsequently. Eaton House Schools cannot be held responsible for any errors unless the employee has informed the school of such changes.

- Anyone working for or acts on behalf of the school must be aware of and comply with the Data Protection Policy and the Privacy Notice which provides further information about how personal data about individuals will be used.

Volunteers and contractors

If you are a volunteer or contractor you will be a data controller in your own right, but the same legal regime and best practice standards set out in this policy will apply to you by law.

Record Keeping

It is important that personal data held by Eaton House School is accurate, fair and adequate. Staff are required to inform the Bursar if they believe that any personal data is inaccurate or untrue or if you are dissatisfied with how it is recorded. This applies to how staff record their own data, and the personal data of others – in particular colleagues, pupils and their parents – in a way that is professional and appropriate.

Staff should be aware of the rights set out below, whereby any individuals about whom they record information on School business (notably in emails and notes) digitally or in hard copy files may have the right to see that information. This absolutely must not discourage staff from recording necessary and sometimes difficult records of incidents or conversations involving colleagues or pupils, in accordance with the schools' other policies, and grounds may sometimes exist to withhold these from such requests. However, the starting position for staff is to **record every document or email in a form they would be prepared to stand by should the person about whom it was recorded ask to see it**.

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 policies and procedures of the school. 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 read and comply with the linked policies mentioned in this document.

Responsible processing also extends to the creation and generation of new personal data and records, which should always be done fairly, lawfully, responsibly and securely.

Care and data security

We require all school staff (and expect all our contractors) to remain mindful of the data protection principles, and to use their best efforts to comply with those principles whenever they process personal information. Data security is not simply an online or digital issue but one that effects daily processes: filing and sending correspondence, notably hard copy documents. Data processors should always consider what the most assured and secure means of delivery is, and what the consequences would be of loss or unauthorised access.

Accidental breaches of the law or this policy in handling personal data will happen from time to time, for example by human error, and will not always be treated as a disciplinary issue. However, failure to report breaches that pose significant risks to the schools or individuals will be considered a serious matter.

We expect all those with management responsibilities to be particular champions of these principles and to oversee the swift reporting of any concerns about how personal information is used by the school to the Principal and Bursar, and to identity the need for (and implement) regular staff training. Staff must attend any training or complete any online training that Eaton House Schools and Dukes Education require them to complete.

Avoiding, mitigating and reporting data breaches

One of the key obligations contained in the General Data Protection Regulation is on reporting personal data breaches. Data controllers must report certain types of personal data breach (those which risk an impact to individuals) to the ICO within 72 hours.

In addition, data controllers should 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, regardless of whether we need to notify the ICO. If staff become aware of a personal data breach, they must notify their Line Manager, IT, and the Bursar. If staff are in any doubt as to whether to report something internally, 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.

As stated above, the school may not need to treat the incident itself as a disciplinary matter – but a failure to report could result in significant exposure for the school, and for those affected, and could be a serious disciplinary matter whether under this policy or the applicable staff member's contract.

Identifying a Data Breach

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data as it can include:

- access by an unauthorised third party
- attacks on a website
- deliberate or accidental action (or inaction) by a controller or processor
- sending personal data to an incorrect recipient
- computing devices (laptops, USB sticks, etc.) or paper records containing personal data being lost or stolen
- accidental destruction of such equipment or files in a fire or flood
- “blagging” offences where information is obtained by deceiving the organisation which holds it
- alteration of personal data without permission
- loss of availability of personal data.

In the context of the above examples, Eaton House Schools, recognises, that there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware.

When a Breach is discovered

It is the responsibility of whoever discovers a breach, or potential breach, to inform their line manager, IT and the Bursar immediately. Full information must be provided, if known, the type of data and the number of data subjects involved. This information must be passed immediately, or, if the breach is discovered outside normal working hours, as soon as possible, to their line manager and Bursar. The ICT Manager and senior management will also be informed immediately to allow for swift action.

Initial Action to be Taken

- Ascertain if the problem is still ongoing and, if so, take the necessary steps to stop the breach from continuing.
- Make an initial assessment of the extent of the breach.

- Senior management, the Bursar and Head of IT will carry out further investigation of the causes and likely impact of the incident.
- Decide if it is of a level of seriousness that requires notification to the ICO (is there a risk to people's rights and freedom?) or the police (has the data been compromised/stolen by a criminal act?).
- Establish whether there is anything that can be done to recover any losses and limit the damage the breach could cause.

If the breach is not reported to the ICO due to being identified as a low/non-existent risk to individual's rights and freedoms associated with a breach and there was remedial action taken immediately after the breach this must still be recorded in the school's data breach register.

Reporting to the ICO

If it is decided that a serious breach has occurred that must be reported to the ICO, the following information will be made available.

- A description of the nature of the personal data breach including, where possible, the categories and approximate number of individuals concerned.
- The categories and approximate number of personal data records concerned.
- The name and contact details of person chosen to liaise with the authorities.
- A description of the likely consequences of the personal data breach
- A description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

It is accepted that not all the necessary checks, or to supply all the required information, within the laid-down 72-hour period is possible. However, it is important that initial contact is made within that period with the ICO. ICO helpline 0303 123 1113.

Persons affected by the data breach must be informed that there has been a data breach, how and when the breach occurred. Also what has been done to correct the situation and what they may need to do to further safeguard themselves. Provide a contact person in order for those affected by the data breach to be able to contact for further information when required.

Training

Eaton House Schools are responsible for training staff and raising awareness of the policies and procedures on the management of personal data under GDPR.

Staff whose main job role is to access and process personal data are trained and kept up to date to be compliant. There are key personnel who would complet the General Data Protection E-Learning course.

All staff receive annual Data Protection Staff Awareness training via the iHasco e-learning platform.

Ongoing training and awareness to all staff is done through staff meetings, insets and policy newsletters which are e-mailed to staff.

New staff receive training on data protection during the induction training before commencing work at the school. New staff are provided the relevant polices relating to the General Data Protection Regulation which they must read and an induction procedures form is signed by the new staff member confirming they have read and understood the policies. They are also required to complete the GDPR UK in Education e-learning certified training course.

Training includes the principles of data protection, procedures to follow if there is a breach and dealing with complaints. All staff are made aware that if they have any questions or concerns relating to data protection they should initially be addressed to the Bursar by emailing: lcorbett@eatonhouseschools.com

Transferring of Information Abroad

Eaton House Schools aims not to transfer personal data outside the UK. On the rare occasion a pupil and their family will move abroad, Eaton House Schools may receive a request from the school the child is moving onto. The information will be transferred to the future school and will be processed appropriately under UK GDPR law.

Status of this Policy

This policy does not form part of the formal contract of employment for staff but it is a condition of employment that staff will abide by the rules and policies made by Eaton House Schools. Any failure to follow the Data Protection Policy may lead to disciplinary proceedings.

Data Security

All employees whose roles involve access to personal data are responsible for ensuring that the data they hold is kept securely and that it is not disclosed, whether accidentally or otherwise, to any unauthorised third party.

All personal data is kept securely on the computer system however there may be times where a hard copy is kept and this should always be securely locked away in a filing cabinet. Personal data on the computer system should be password protected both on a local hard drive and on a network drive that is regularly backed up. Only authorised staff may access employee's personal data.

Any unauthorised disclosure will normally be regarded as a disciplinary matter, and may be considered gross misconduct in some cases.

Eaton House Schools do not normally share personal data without consent, however there are some circumstances where this maybe necessary. This includes:

- An issue with a pupil/parent/carer that puts our staff at risk
- The need to liaise with other agencies (consent is necessary prior to this)
- Suppliers and contractors need data to enable us to provide services for our staff and pupils e.g. IT companies.

Eaton House Schools ensure that they only appoint suppliers and contractors that provide sufficient guarantees that they comply with UK GDPR law. A contract with the supplier or contractor is drawn up to ensure the fair and lawful processing of personal data we share and that it is only shared to enable us to carry out our services.

Subject Consent

The Data Protection Act 2018 and GDPR sets a high standard for consent and requires a positive opt-in. As well as keeping evidence of any consent, the school ensures that people can easily withdraw consent. This can be done by e-mailing the school.

It should be noted, however, that consent is only one of the lawful bases on which data processing depends. In brief, the others include the following.

- Contract: if processing someone's personal data is necessary to fulfil the organisation's contractual obligations to them.
- Legal obligation: if processing personal data is necessary to comply with a common law or statutory obligation.
- Vital interests: refers to processing personal data to protect someone's life.

- Legitimate interests: applies when data is used in ways people would reasonably expect and which have a minimal privacy impact, or where there is a compelling justification for the processing.

Note that the GDPR provides for special protection for children's personal data and Eaton House Schools will comply with the requirement to obtain parental or guardian consent for any data processing activity involving anyone under the age of 16.

Rights of Individuals

In addition to the schools' responsibilities when processing personal data, individuals have certain specific rights, perhaps most significantly that of access to their personal data held by a controller (i.e. the schools). This is known as the 'subject access right' (or the right to make 'subject access requests'). Such a request must be dealt with promptly and does not need any formality, nor to refer to the correct legislation. If you become aware of a subject access request (or indeed any communication from an individual about their personal data), you must tell the Bursar 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; and
- 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.

None of the above rights for individuals are unqualified and exceptions may well apply. However, certain rights are absolute and must be respected, specifically the right to:

- object to automated individual decision-making, including profiling (i.e. where a significant decision is made about the individual without human intervention);
- object to direct marketing; and
- withdraw one's consent where we are relying on it for processing their personal data (without affecting the lawfulness of processing carried out prior to that point in reliance on consent, or of any processing carried out on some other legal basis other than consent).

In any event, however, if you receive a request from an individual who is purporting to exercise one or more of their data protection rights, you must tell the Bursar as soon as possible.

Subject Access Requests (SARs)

An employee or parent may request details of personal information which Eaton House Schools holds about him or her under GDPR. If an individual would like a copy of the information held on him or her, they should write to the Bursar or email at: lcorbett@eatonhouseschools.com.

The requested information will be provided within one month of the date of receipt of the request. If there is any reason for delay, this will be communicated within the four-week period. If the SAR is considered complex, an extension may be considered and we aim to comply within three months of receipt of the request. There is no charge of a fee unless the request proves to be "manifestly excessive or repetitive". If the school does find it necessary to charge a fee, it would be based on the administrative cost of providing the information.

Personal data about a child belongs to that child and not the child's parents or carers. In order for a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a SAR, or have given their consent.

Children under the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a SAR. Therefore most SARs may be granted without the express permission of the pupil judged on a case-by-case basis.

We may not disclose information if:

- It may cause serious harm to the pupil or an individual
- Reveals if the child has been abused or at risk of abuse
- Includes another person's personal data where we cannot reasonably anonymise
- Is part of sensitive documents related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references or exam scripts.

SARs Requests by Staff

Staff should inform the Head of HR (hr@eatonhouseschools.com) at the earliest opportunity if they believe that any of their personal data is inaccurate.

In the event of a disagreement between an employee and Eaton House Schools regarding personal data, the matter should be taken up under Eaton House Schools' formal grievance procedure.

Where an employee makes a request for access to their personal data which is manifestly unfounded or excessive, particularly when requests are repetitive, a reasonable fee can be charged. The fee is based on the administrative cost of providing the information.

The Head of HR informs staff, when their employment commences, that it is their responsibility to inform HR if there are any changes to their personal details.

Data Accuracy and Security

The school will endeavour to ensure that all personal data held in relation to an individual is as up to date and accurate as possible. In relation to staff, individuals must notify the HR department in writing (an email will suffice), of any changes to the information held about them. In relation to pupils, parents and carers must update their personal data in the Parent Portal via their personal log-in details. The Data Manager, will check and confirm the data request change.

An individual has the right to request that any inaccurate or out-of-date information about them is erased or corrected. There are exemptions to this, which falls under the law.

The school will take appropriate technical and organisational steps to ensure the security of personal data about individuals, including policies around use of technology and devices, and access to school systems. All staff and senior management will be made aware of this policy and their duties under Data Protection Law and receive relevant training.

CCTV

We use CCTV in various locations around the school site to ensure it remains safe. We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs informing that CCTV is in use.

Queries and Complaints

If an individual believes that the school has not complied with this policy or acted otherwise than in accordance with Data Protection Law, they should utilise the school Complaints Procedure and should also notify the school office. A complaint can be lodged with the Information Commissioner's Office (ICO), although the ICO recommends that steps are taken to resolve the matter with the school before involving the regulator.