**WINDLESHAM HOUSE SCHOOL**

**DATA PROTECTION POLICY**

**Contents**



## 1. Policy Statement

1.1 Windlesham House School (the "School") is part of the Charterhouse Schools Group. Its ICO registration number is Z6092852 and its registered address is Charterhouse School, Charterhouse, Godalming, Surrey GU7 2DX. The School is a registered charity and its charity number is 312054

1.2 Staff are advised to familiarise themselves with this policy and its associated procedures including Data Privacy Notice(s), CCTV Procedure, Procedure on the use of Images and Videos, Retention of Documents, Data Breach Reporting Procedure, Subject Access Request Procedure.

1.3 This policy aims to ensure that the school's staff and representatives get data protection right and that careful thought is given to data protection issues. This means handling all personal information fairly, lawfully, securely and responsibly.

1.3 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?

1.4 A summary of key actions for staff under the policy is provided at Appendix 1.

## 2. Background

2.1 During the course of the School's activities it collects, stores and processes personal data (sometimes sensitive in nature) about staff, pupils, their parents, its contractors and other third parties (in a manner more fully detailed in the School's Privacy Notices). The School, as "data controller", is liable for the actions of its staff and governors in how they handle data.

2.2 UK data protection law consists primarily of the UK version of the General Data Protection Regulation (the GDPR) and the Data Protection Act 2018 (DPA 2018). The DPA 2018 includes specific provisions of relevance to independent schools: in particular, in the context of our safeguarding obligations, and regarding the right of access to personal data.

2.3 Data protection law has in recent years strengthened the rights of individuals and placed tougher compliance obligations on organisations including schools that handle personal information. The Information Commissioner's Office (ICO) is responsible for enforcing data protection law and will typically look into individuals' complaints routinely and without cost and has various powers to take action for breaches of the law.

2.4 The School also recognises that the risk to data subjects is not only legal but reputational, operational and potentially safeguarding related.

## 3. Definitions

Key data protection terms used in this data protection policy are:

- **Data controller** – a person or body that determines the purpose and means of the processing of personal data, and who is legally responsible for how it is used. For example, the School (including by its governors) is a controller. An independent contractor who makes their own such decisions is also, separately, likely to be a data controller.

- **Data processor** – an organisation that processes personal data on behalf of a data controller, for example a payroll or IT provider or other supplier of services with whom personal data may be shared but who is not authorised to make any decisions about how it is used.

- **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 information (or 'personal data'):** any information relating to a living individual (a data subject) by which that individual may be identified by the controller. That is not simply a name but any form of identifier, digital or contextual, including unique ID numbers, initials, job titles or nicknames. Note that personal information will be created almost constantly in the ordinary course of work duties (such as in emails, notes of calls, and minutes of meetings). The definition includes expressions of opinion about the individual or any indication of the School's, or any person'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. There are also separate rules for the processing of personal data relating to criminal convictions and offences.

## 4. Application of this policy

4.1 This policy sets out the School's expectations and procedures with respect to processing any personal data we collect from data subjects (including parents, pupils, employees, alumni, contractors and third parties).

4.2 Those who handle personal data as employees or governors of the School are obliged to comply with this policy when doing so. For employees, breaches of this policy may result in disciplinary action. 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 School or individuals will be considered a serious matter. All governors are also required to follow this policy and attend relevant training as part of their oversight duties.

4.3 In addition, this policy represents the standard of compliance expected of those who handle the School's personal data as contractors, whether they are acting as "data processors" on the School's behalf (in which case they will be subject to binding contractual terms) or as data controllers responsible for handling such personal data in their own right.

4.4 Where the School shares personal data with third party data controllers – which may range from other schools, to parents, to appropriate authorities, to casual workers and volunteers – each party will need a lawful basis to process that personal data and will be expected to do so lawfully and with due regard to security and confidentiality, as set out in this policy.

4.5 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.

## 5. Person responsible for Data Protection at the School

The School has appointed the Director of Finance and Operations (DFO) as the Privacy and Compliance Officer who will endeavour to ensure that all personal data is processed in compliance with this notice and Data Protection Law.

The Director of Finance and Operations can be contacted by:
a. Emailing - dfo@charterhouse.org.uk
b. Telephoning – 01483 291500
c. Writing to Director of Finance and Operation at Charterhouse, Godalming, Surrey, GU7 2DX.

## 6. The Principles

6.1 The GDPR sets out six principles relating to the processing of personal data which must be adhered to by data controllers (and data processors). These require that 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.

6.2 The GDPR's broader '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 by way of logs and policies;
- documenting significant decisions and assessments about how we use personal data
- generally having an 'audit trail' vis-à-vis data protection and privacy matters, including for example when and how our Privacy Notice(s) were updated; when staff training was undertaken; how and when any data protection consents were collected from individuals; how personal data breaches were dealt with, whether or not reported (and to whom), etc.

## 7. Lawful grounds for data processing

7.1 Under the GDPR there are several different lawful grounds for processing personal data. One of these is consent. Given the relatively high bar of what constitutes consent under GDPR (and the fact that it can be withdrawn by the data subject) the school will always consider if there is another lawful ground on which to process personal data where possible.

7.2 One of these alternative grounds is 'legitimate interests', which is the most flexible basis for processing. However, it does require transparency and a balancing assessment between the rights of the individual and the interests of the School. It can be challenged by data subjects and also means the School is taking on extra responsibility for considering and protecting people's rights and interests. The School's legitimate interests are set out in its Privacy Notice, as GDPR requires.

7.3 Other lawful grounds include:

- compliance with a legal obligation, including in connection with employment, engagement of services and diversity;
- contractual necessity, e.g. to perform a contract with staff or parents, or the engagement of contractors;
- a narrower set of grounds for processing special categories of personal data (such as health information), which includes explicit consent, emergencies, specific public interest grounds or processing required to safeguard children and vulnerable individuals.

## 8. Headline responsibilities of all staff

### 8.1 Record-keeping

8.1.1 It is important that personal data held by the School is accurate, fair and adequate. Staff are required to inform the School 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.

8.1.2 Staff must also report outdated personal data they come across in any format, including in legacy systems and paper archives.

8.1.3 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 School's 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.

### 8.2 Data handling

8.2.1 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 all relevant School policies and procedures (to the extent applicable to them). In particular, there are data protection implications across a number of areas of the School's wider responsibilities. All staff should read and comply with such school policies and procedures including Child Protection and Safeguarding, Online Safety, Data Privacy Notice(s), CCTV Procedure, Procedure on the use of Images and Videos, Data Breach Reporting Procedure, Subject Access Request Procedure.

8.2.2 Staff should avoid using personal devices to store or transmit personal data related to school business until explicitly authorised and encrypted.

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

### 8.3 Avoiding, mitigating and reporting data breaches

8.3.1 One of the key obligations contained in the GDPR 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.

8.3.2 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, regardless of whether we need to notify the ICO. If staff become aware of a personal data breach they must notify the [DEL:Data Privacy Manager] [INS:Director of Finance and Operations], 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.

8.3.3 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.

**8.4 Care and data security**

8.4.1 More generally, we require all School staff (and expect all our contractors) to remain mindful of the data protection principles (see section 3 above), 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 handlers should always consider what they most assured and secure means of delivery is, and what the consequences would be of loss or unauthorised access.

8.4.2 We expect all those with management / leadership 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 [DEL:Data Privacy Manager] [INS:Director of Finance and Operations]. Staff must attend any training on data protection that the School requires them to.

## 9. Rights of Individuals

9.1 In addition to the School's responsibilities when processing personal data, individuals have certain specific rights, perhaps most significantly that of access to their personal data held by a data controller (i.e. the School). 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 [DEL:Data Privacy Manager] [INS:Director of Finance and Operations] as soon as possible.

9.2 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.

9.3 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).

9.4 All requests under data protection rights must be logged in the Subject Access Request log, available via the Director of Finance and Operations. Staff must not respond independently without authorisation.

## 10. Data Security: online and digital

10.1 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.

10.2 We will put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Security procedures include:

- **Entry controls.** Any stranger seen in entry-controlled areas should be reported to Reception immediately.

- **Secure lockable desks and cupboards.** Staff are advised to keep desks and cupboards locked if they hold confidential information of any kind. (Personal information is always considered confidential.)

- **Methods of disposal.** Paper documents should be shredded. Digital storage devices should be physically destroyed when they are no longer required. IT assets must be disposed of in accordance with the Information Commissioner's Office guidance on the disposal of IT assets. All hard drives should be securely wiped before being recycled.

- **Equipment.** Data users must ensure that individual monitors do not show confidential information to passers-by and that they lock their PC when it is left unattended.

- **Working away from the school premises – paper documents.** Paper documents must be removed from vehicles once the destination has been reached and secured immediately. Staff should take care to keep documents together, out of public areas and in a secure area and to return them to Windlesham House as soon as possible

- **Working away from the school premises – electronic working.** Staff can access school files via Remote Desktop, and cloud-based services. Use of these platforms must be in accordance with the Staff Acceptable Use Policy.

- **Document printing.** Documents containing personal data must be printed via the automatic print queue and released when needed in-person – not left on photocopiers/printers unattended.

- **File Security.** Network access permissions are in place to ensure that only appropriate stakeholders are able to access confidential files. Users must ensure that files containing personal data are stored in the correct area of the network.

- **File Sharing.** Care must be taken to ensure that files containing personal data are shared using the most secure method possible. When necessary to share any bulk personal data, files must be encrypted and password-protected. The passwords must not be shared via the same medium as transfer.

- **File Storage.** Files containing personal data should be deleted when no longer needed, in line with GDPR regulations.

- **Account Security.** Data users will not share user credentials with any other users and must report any suspected breach of account security to IT.

- **Security Printing**. All confidential documents must be collected promptly from printers using a secure print release function.

- **Use of Cloud Services**. Only approved cloud platforms may be used for storing and sharing personal data.

10.3 Any member of staff found to be in breach of the above security measures may be subject to disciplinary action.

## 11. Data Breaches

11.1 Please act promptly to report any data breaches following the Data Breach Reporting Procedure.

11.2 The School will maintain a data breach log and report high-risk breaches to the ICO and affected individuals as required under Articles 33 and 34 of the UK GDPR.

## 12. Policy Review

This policy and its associated procedures will be updated as necessary to reflect best practice and to ensure compliance with any changes or amendments. The policy will formally be reviewed by the Governing Body every two years.

**Appendix 1 – Key Data Protection Facts**

- You must report and suspected or actual breach of personal data security
- Do not share passwords or leave devices unlocked
- Dispose of personal data securely – shred paper documents or dispose in confidential waste sacks and securely delete files
- Be cautious with WhatsApp or messaging apps – do not use them for sharing sensitive personal data
- Refer all Subject Access Requests and other rights requests to the Data Privacy Manager

| | Data Protection Facts | Remarks |
|---|---|---|
| 1 | **Personal data** includes information such as names, addresses, email addresses, financial details, images and education and employment details | The School has legitimate interests for holding the minimum amounts of personal information to educate pupils and employ staff. It must be stored securely. |
| 2 | **Sensitive Personal data** includes information such as physical and mental health, ethnicity & diversity, political or religious views, trade union membership, or criminal records | This data must be held separately and securely. Access must be limited to the minimum number of people that have a business need for the information |
| 3 | **Security Principles:**<br>• Only collect and hold the minimum amount of personal data to undertake school activities<br>• Sensitive Data, taking data outside the UK, and publishing a pupil image and name requires **CONSENT**<br>• Only retain personal data in line with the School Records Retention Policy<br>• Internal sharing of personal data should be minimised<br>• External sharing of personal data is not allowed without authority of the Privacy Manager<br>• All school electronic devices must be password protected<br>• Electronic personal data must be held in a restricted area with limited access<br>• Hard copies must be held securely | This should be gained on initial data collection forms<br><br>Unless government or law enforcement agencies<br>Including memory sticks<br>Information should only be shared with those who need it to complete their job |
| 4 | **Personal Data in School**<br>• Should be held in one secure and restricted location | |

| | | |
|---|---|---|
| | ○ Staff info – HR files, Sage<br>○ Prospective Pupil info - Admissions, ISAMS<br>○ Pupil info – Academic matters ISAMS and Pastoral Matters with Head of Houses and Tutors<br>○ Safeguarding info – DSL and My Concern<br>○ Parent general info – ISAMS<br>○ Financial info – Finance<br>○ Medical info – isams, Medi, Matrons<br>○ Images – Marketing<br>• Holding paper copies should be minimised and must be kept securely<br>• Bulk personal data (more than 2 people) should be distributed by hyperlink if possible or by a password protected file if not<br>• Passage of personal data by emails should be minimised and deleted after 18 months | Saving personal data outside these areas is only allowed with permission of the Bursar<br><br>If used at meetings it must be collected afterwards<br><br>Data required after 18 months should be saved as set out above |
| 5 | **Personal Data outside School**<br>• Personal data outside School should be minimised<br>• Data must be held on a password protected devices or hard copies held securely<br>• Bulk transfer of personal data must be password protected<br>• Communications with parents on personal data matters should be via ISAMS or parent portal | Where possible it should be accessed via SharePoint |