

I. Background

Data protection is an important legal compliance issue for Holy Cross Prep School. During the course of the School's activities it collects, stores and processes personal data (sometimes sensitive in nature) about staff, pupils, their parents, suppliers and other third parties (in a manner more fully detailed in the School's Privacy Notice. It is therefore an area where all staff have a part to play in ensuring we comply with and are mindful of our legal obligations, whether that personal data is sensitive or routine.

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.

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.

Those who are involved in the processing of personal data are obliged to comply with this policy when doing so. Accidental breaches will happen and may not be a disciplinary issue, but any breach of this policy may result in disciplinary action. This policy may be amended at any time.

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

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

- Data controller – an organisation that determines the purpose and means of the processing of personal data. For example, the School is the controller of pupils' 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. All data processors engaged by the School are subject to appropriate due diligence, written contracts, and ongoing compliance checks to ensure they meet data protection requirements.
-
- 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), including name, initials, job title, 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, including the GDPR. 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. There are also separate rules for the processing of personal data relating to criminal convictions and offences.

2. Data Protection Lead

The School Bursar will deal with all your requests and enquiries concerning the school's uses of personal data and 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 the Bursar.

3. The 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). 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.

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 by way of logs and policies;
- documenting significant decisions and assessments about how we use personal data; and
- 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, how and when data protection consents were collected from individuals, how breaches were dealt with, etc.

The School retains personal data only for as long as is necessary to fulfil the purposes for which it was collected, including to meet legal, regulatory, safeguarding and operational requirements. Retention periods are determined in accordance with statutory guidance and best practice for independent schools and are set out in the School's Data Retention and Disposal Policy.

When personal data is no longer required, it is securely deleted or destroyed in a timely manner, ensuring confidentiality is maintained. Staff must follow the School's procedures for storing, archiving and disposing of records to ensure compliance with data protection law.

4. Lawful grounds for data processing

Under the GDPR there are several different lawful grounds for processing personal data. One of these is consent. However, because the definition of what constitutes consent has been tightened under GDPR (and the fact that it can be withdrawn by the data subject) it is generally considered preferable to rely on another lawful ground where possible.

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 Controller. It can be challenged by data subjects and also means the Controller 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 Policy, as GDPR requires.

Other lawful grounds include:

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

Data Protection Impact Assessments (DPIAs)

The School will carry out a Data Protection Impact Assessment (DPIA) where processing of personal data is likely to result in a high risk to individuals' rights and freedoms. This includes, for example, the introduction of new technologies, large-scale processing of personal data, or the processing of sensitive (special category) data.

A DPIA will assess the nature, scope, context and purposes of the processing, identify and evaluate risks to individuals, and set out measures to mitigate those risks. DPIAs will be reviewed and approved by the Data Protection Lead (Bursar) prior to the commencement of the relevant processing activity.

Staff must consult the Data Protection Lead at an early stage when planning any new project or process involving personal data to determine whether a DPIA is required.

5. Headline responsibilities of all staff

Record-keeping

It is important that personal data held by the School is accurate, fair and adequate. You are required to inform the School if you believe that *your* personal data is inaccurate or untrue or if you are dissatisfied with the information in any way. Similarly, it is vital that the way you record the personal data of others – in particular colleagues, pupils and their parents – is accurate, professional and appropriate.

Staff should be aware of the rights set out below, whereby any individuals about whom they record information in emails and notes on School business 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 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.

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 all relevant

DATA PROTECTION POLICY

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 read and comply with the following policies:

- Safeguarding and Child Protection Policy
- Acceptable Use of Technology and e-Safety Policy
- Taking, Storing and Using Images of Children Policy
- Personal Data Breach Procedure
- Data Retention and Disposal Policy
- Privacy Notice
- Staff Privacy Notice

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.

Staff Training and Awareness

The School ensures that all staff receive appropriate data protection training to enable them to handle personal data safely and in accordance with legal requirements.

- All new staff receive data protection training as part of their induction.
- Refresher training is provided regularly, and whenever there are significant updates to legislation, guidance or School policies.
- Training is tailored to staff roles and responsibilities, with additional guidance provided where staff handle more sensitive data or specific processes such as subject access requests or data breaches.
- The Data Protection Lead (Bursar) and relevant senior staff receive enhanced training to support their responsibilities.
- Records of training are maintained, and compliance is monitored by the School.

The School also promotes ongoing awareness through regular updates, guidance and access to relevant policies to ensure data protection forms part of everyday practice.

Avoiding, mitigating and reporting data breaches

One of the key new 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. Please refer to the Personal Data Breach Procedure for further information.

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 you become aware of a personal data breach you must notify the Bursar. 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.

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 staff member's contract.

Care and data security

More generally, we require all School staff to remain conscious of the data protection principles (see section 3 above), to attend any training we require them to, 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 affects daily processes: filing and sending correspondence, notably hard copy documents. Staff should always consider what their 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 about how personal information is used by the School to the Bursar, and to identify the need for (and implement) regular staff training.

6. Rights of Individuals

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 Headteacher or 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;
- 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.

Except for the final bullet point, none of these rights for individuals are unqualified and exceptions may well apply. 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 Headteacher or the Bursar as soon as possible.

7. Data Security: online and digital

The School ensures 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. Please refer to the Acceptable Use of IT Policy. As such, no member of staff is permitted to remove personal data from School premises, whether in paper or electronic form and wherever stored,

without prior consent of the Head or Bursar. Where a worker is permitted to take data offsite it will need to be encrypted. Use of personal email accounts or unencrypted personal devices for official School business is not permitted.

8. Data Protection Complaints Procedure

The School is committed to handling data protection complaints fairly, effectively and in line with UK data protection law and guidance from the Information Commissioner's Office (ICO).

8.1 How to Make a Complaint

Any individual (including parents, pupils, staff, or third parties) can raise a data protection complaint by contacting the School via:

- Email: secretary@holycrossprep.com
- In writing: Holy Cross Preparatory School, George Road, Kington upon Thames KT2 7NU
- For the attention of: The Bursar (Data Protection Lead)

8.2 Acknowledgement

The School will acknowledge all data protection complaints within 30 calendar days of receipt.

8.3 Investigation

The Bursar (or delegated senior leader) will:

- Review the nature of the complaint
 - Gather relevant information
 - Make necessary enquiries
 - Keep the complainant informed
- All complaints will be handled without undue delay.

8.4 Outcome

The School will provide a written outcome including:

- Summary of findings
- Actions taken
- Improvements made
- ICO escalation rights

8.5 Record Keeping

The School will maintain a record including:

- Date received
- Acknowledgement issued
- Complaint details
- Communications
- Outcome
- Actions taken

8.6 Governance and Monitoring

The School will review complaints regularly and report themes to the governing body.

9. 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?

Data protection law is therefore best seen not as oppressive red tape, or a reason not to do something necessary or important, but a code of useful and sensible checks and balances to improve how to handle and record personal information and manage our relationships with people. This is an important part of the School's culture and all its staff and representatives need to be mindful of it.

Appendix I - Email security: guidelines for sending personal data safely (Source: The Key)

Account settings

Enable settings that prevent contact addresses from auto-filling. This means it will be more difficult to accidentally send emails to the wrong person. Enable settings that require staff to manually confirm they want to send an email, as a precaution against the ease of sending emails accidentally.

Use password protection

When attaching a document that contains personal data to an email, enable password protection on the document.

Check the recipient's security arrangement

Check that the security arrangements of recipients are secure enough before sending them an email with personal data in it.

Think about whether you should hide recipients' email addresses

If you're sending an email to a group of people, consider whether the recipients should know each other's email addresses. If it's not appropriate for them to know then you should blind carbon copy ('bcc') the recipients. By using 'bcc', their email address cannot be seen by other recipients. If you carbon copy ('cc') a recipient, their email address is visible to everyone else who receives the email.

Appendix 2 – Saving Correspondence

It is important that all correspondence regarding pupils or parents is saved in a structured and organised way on the Records drive to enable ease of reference/retrieval.

Information, such as emails, notes of calls or minutes of meetings, is defined as personal data and regulated by data protection laws, and individuals have the right to request this information, known as a Subject Access Request.

You should save, as you go, anything in relation to a pupil regarding important issues or potential concerns that may arise in the future. This includes expressions of opinion about the individual or any indication of someone's intentions towards that individual.

- The recipient should save the correspondence onto the Records drive (including their responses).
- The MEDICAL folder is for forms such as inhaler, Epipen or antibiotics permission or intimate care. Any correspondence relating to medical and dietary should be saved in correspondence with a descriptive title, e.g. dietary, to help identify these records.
- All correspondence (important letters, emails, notes in homework diaries) that need to be kept by admin/teachers are to be filed as follows:
 - Save in Records drive / Year group / Class / Pupil name / Current class
 - Correspondence then ADMIN or TEACHER folder or MEDICAL (i.e. intimate care form)
 - If no admin / teacher / medical folder – please make up one (new pupils will have these)
 - Save and rename using the format: 'date title' – and parents email title if different i.e. 181016 collection arrangements – pick up for first name surname
 - Shred / delete original source

Appendix 3 - Remote Access RDS (Remote Desktop Service)/EMAIL

This guidance relates to best practice for accessing the school system, both in terms of email and via the remote logon server (RDS), from outside the school network and personal devices used. Please also refer to the Acceptable Use of Technology and e-Safety Policy.

Protection with software updates:

Windows 10/Office Updates - each month Microsoft circulates patches for their software products, check to make sure these patches/updates are being applied correctly. Windows 7, 8 and 8.1 are still supported by Microsoft but these operating systems are coming to the end of life as is early editions of Windows 10. To check compatibility: [Windows lifecycle fact sheet](#)

Applications – software that you are running on your device needs to be legitimate and kept up to date. Applications such as Java or Flash unpatched can introduce security risks, if you have these installed on your system when were they last updated?

Security - with the exception of iOS 12+ (iPhone/iPad), the device that you are using must be secured with an up to date working Antivirus/Security product, such as Sophos, Kaspersky or Bitdefender.

Apple - is your device still supported and receiving updates? You can check the unsupported device list [here](#), equally iPhone/iPads if it's unsupported it's not safe for school use.

Android/Google - if the device is no longer receiving updates via the "Play Store" it is most likely unsupported and not fit for use.

Personal Data Breach :

Raise concerns that you may have with SLT.

Under no circumstance should school data be downloaded and stored on a personal device, if the device was lost, stolen or even hacked this would trigger a data breach.

Report all data breach's correctly, using the correct school protocols. Please refer to the Personal Data Breach Procedure.

Don't share your user details, under no condition should you be sharing your passwords/accounts with a colleague or a friend.

Passwords are rotated for good reasons, colleagues should use a logical method of remembering them, writing them on post attached to your monitor is not acceptable - a password manager would be best, there are many.

Don't use public wireless networks to access school information, public networks are often targeted by criminal gangs.

Discard personal digital devices correctly, if it's capable of storing digital content, it will need to be recycled and scraped correctly.

Best Practice:

- # Protect your family, ask your ISP about parental locks, do you know what is being accessed on the internet from your home?
- # Protect yourself, use social media cautiously, companies such as Facebook have fine-tuned their operations to manipulate your time online.
- # Phishing scams, if you're unsure or have questions about the sender of an email/SMS, raise your concerns with your service provider or delete the message.
- # Safeguard your home network, ask your ISP about free router/service upgrades.
- # Digital mediums such as CD/DVD or hard drive(s) have a shorter life time than stone, papyrus or paper. If it's working today, it's unlikely that to be working in the distant future, having a working backup is a good idea.
- # Keep it simple, having less is always best.
- # When not in use, disable, delete or uninstall.

Appendix 4 - How to keep personal data safe (Source: The Key)

Also refer to the Acceptable Use of Technology and e-Safety Policy.

DO:

- ✓ **Remember that data protection laws DO NOT stop you from reporting safeguarding concerns**
 - You must still report to the relevant people where you're concerned about a child. You do not need anyone's consent to do this
- ✓ **Only collect the information you actually need**
 - When you're requesting information (for example, via consent forms, admissions forms or surveys) ask yourself "Do I really need this? What will I actually use it for?"
 - If you don't need it, or only want it "just in case", don't collect it
 - If you've already collected personal information that you don't need, delete it
- ✓ **Keep personal data anonymous, if possible**
 - For example, if you're emailing a colleague about accommodating a pupil's religion, or about managing a pupil's medical condition, don't name the child if you don't need to
 - This is particularly important with photographs for external use – if you have an image of a child, don't attach their name to it unless you have explicit consent to do so
- ✓ **Think before you put information up on the wall**
 - If your display is an essential part of teaching and learning, or helps to keep pupils safe, it's fine. This might include medical information, or a list of parents' evening appointments. Still only display the information you really need to
 - If your display is non-essential, promotional, or there might be a safeguarding risk, either ask the pupil or parents for consent first or just don't display it
- ✓ **Take care when you're taking personal information home with you**
 - Keep physical documents in a secure, closed folder along with your contact details in case the folder is lost
 - Store the documents in a safe place at home – don't leave them in your car or at a friend's house
- ✓ **Practise good ICT security**
 - Passwords should be at least 7 characters, with upper and lower-case letters and special characters
 - Password-protect documents and email attachments that include personal data
 - Always double-check that you're emailing personal data to the correct person, who is authorised to see it
 - Use 'bcc' when you're emailing a group of people who don't have email addresses for everyone else in the group, e.g. parents or volunteers

DON'T:

× Leave personal data out on your desk

- Keep your desk clear, so people cannot see information about others accidentally. The same goes for personal data written on post-it notes, on top of the printer, or on an unattended computer screen

× Take any sensitive personal information home with you

- If the information is confidential, sensitive or risky, it's best to leave it on the school site or computer system, where there are security measures and processes in place

Report to the Bursar immediately if you think personal data has been lost, stolen or wrongly disclosed so we can quickly take steps to mitigate the impact of the breach.

You should also speak to the Bursar if:

- You have any concerns at all about keeping personal data safe
- You're introducing a new process or policy that involves using personal data
- Anyone asks you to see the data that we have about them. This is called a 'subject access request', and the person will be entitled to this information