Data Protection Policy

July 2025

DATA PROTECTION POLICY

1. Background

Data protection is an important legal compliance issue for King's College School and Wimbledon Common Preparatory School (the "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, 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. 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 handling is sensitive or routine.

UK data protection law consists primarily of the UK version of the General Data Protection Regulation (the "UK 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 in the UK and will typically look into individuals' complaints routinely and without cost, and has various powers to take action for breaches of the law.

2. 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 controller.

- **Data Processor** – an organisation that processes personal data on behalf of a 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 data, 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.

3. Application of this policy

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, contractors and third parties).

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 which could amount to gross misconduct and result in summary dismissal.

A member of staff who deliberately or recklessly discloses Personal Data held by the school without proper authority may also be guilty of a criminal offence under s170 of the Data Protection Act 2018.

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 'processors' on the school's behalf (in which case they will be subject to binding contractual terms) or as controllers responsible for handling such personal data in their own right.

Where the school shares personal data with third party controllers – which may range from other schools to parents and appropriate authorities – 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.

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.

4. Person responsible for Data Protection at the School

The school has appointed Judicium as the Data Protection Officer who will endeavour to ensure that all personal data is processed in compliance with this policy and the principles of applicable data protection legislation. Their contact details are:

Judicium Consulting Limited
Address: 72 Cannon Street, London, EC4N 6AE
Email: dataservices@judicium.com
Web: www.judiciumeducation.co.uk
Telephone: 0345 548 7000 option 1 then option 1 again

4.1 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 who has primary and day to day responsibility for implementing this policy, working in conjunction with the DPO as appropriate who is responsible for overseeing this Data Protection Policy, helping develop data-related policies and guidelines, dealing with any queries on their interpretation, and advising on any data protection matters including data breaches and Subject Access Requests (SARs).

Please contact the bursar with any questions about the operation of this Data Protection Policy or the UK GDPR or if you have any concerns that this policy is not being or has not been followed at bursar@kcs.org.uk. In particular, you must always contact the bursar in the following circumstances:

(a) If you are unsure of the lawful basis being relied on by the school to process personal data;

(b) If you need to rely on consent as a fair reason for processing, please see the lawful grounds for data processing section:

(c) If you need to draft privacy notices or fair processing notices;

(d) If you are unsure about the retention periods for the personal data being processed, but please refer to the school's *Information and records retention policy* in the first instance];

(e) If you are unsure about what security measures need to be put in place to protect personal data;

(f) If there has been a personal data breach, but please refer to the school's *Data breach policy* and *Information security policy*;

(g) If you are unsure on what basis to transfer personal data outside the EEA;

(h) If you need any assistance dealing with any rights invoked by a data subject;

(i) Whenever you are engaging in a significant new (or a change in) processing activity which is likely to require a data protection impact assessment or if you plan to use personal data for purposes other than what it was collected for;

(j) If you plan to undertake any activities involving automated processing or automated decision making.

(k) If you need help complying with applicable law when carrying out direct marketing activities;

(l) If you need help with any contracts or other areas in relation to sharing personal data with third parties.

5. The principles

The UK GDPR sets out six principles relating to the processing of personal data which must be adhered to by controllers (and 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 UK 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 (including via formal risk assessment documents called Data Protection Impact Assessments ("DPIA")); 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; 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.

6. Lawful grounds for data processing

Under the UK GDPR there are several different lawful grounds for processing personal data. One of these is consent. However, given the high bar of what constitutes consent under the UK GDPR (and the fact that it can be withdrawn by the data subject) it is considered preferable for the school 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 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 the UK GDPR requires.

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, and specific public interest grounds.

7. Headline responsibilities of all staff

Record-keeping

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.

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 making necessary and sometimes difficult records of incidents or conversations involving colleagues or pupils and parents, 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**.

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 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 such as safeguarding and IT security, so all staff should read and comply with the following policies:

- Information and Record Retentions Policy
- Information Security Policy
- Data Breach Policy

- Privacy Notices
- Guidance for Staff on the Use of Photos and Videos of Pupils
- CCTV policy

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.

Avoiding, mitigating, and reporting data breaches

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

In addition, 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 bursar or the support services and compliance officer. 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.

If you know or suspect that a personal data breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the bursar or support services and compliance officer and email a completed data breach report form (see Appendix 2 of the data breach policy – a word version of the form is also available in the staff handbook on SharePoint) to them.

Care and data security

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.

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 identity the need for (and implement) regular staff training. Staff must attend any training we require them to.

Use of third party platforms / suppliers

As noted above, where a third party is processing personal data on the school's behalf it is likely to be a data 'processor,' and this engagement must be subject to appropriate due diligence and contractual arrangements (as required by the UK GDPR). It may also be necessary to complete a DPIA before proceeding – particularly if the platform or software involves any sort of novel or high-risk form of processing (including any use of artificial intelligence ("AI") technology). Any request to engage a third-party supplier should be referred to Kelly Brown, support services and compliance officer in the first instance, and at as early a stage as possible.

The school will generally not share personal data with third parties unless certain safeguards and/or contractual arrangements have been put in place. The following points will be considered:

- Whether the third party has a need to know the information for the purposes of providing the contracted services:
- Whether sharing the personal data complies with the privacy notice that has been provided to the data subject and, if required, the data subject's consent has been obtained;
- Whether the third party has agreed to comply with the required data security standards, policies and procedures and implemented adequate security measures;
- Whether the transfer complies with any applicable cross border transfer restrictions.

There may be circumstances where the school is required either by law or in the best interests of our pupils, parents, or staff to pass information onto external authorities for example, the Local Authority, the Independent Schools Inspectorate, the Charity Commission, or the Department of Education. These authorities are up to date with data protection law and have their own policies relating to the protection of any data that they receive or collect.

Transfer of Data Outside the European Economic Area (EEA)

The UK GDPR restricts data transfers to countries outside the EEA to ensure that the level of data protection afforded to individuals by the UK GDPR is not undermined.

The school will not transfer data to another country outside of the EEA without appropriate safeguards being in place and in compliance with the UK GDPR. All staff must comply with the school's guidelines on transferring data outside of the EEA. For the avoidance of doubt, a transfer of data to another country can occur when you transmit, send, view or access that data in that particular country.

Transfer of Data Outside the UK

The school may transfer personal information outside the UK and/or to international organisations on the basis that the country, territory, or organisation is designated as having an adequate level of protection. Alternatively, the organisation receiving the information has provided adequate safeguards.

8. 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 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 bursar as soon as possible. For further details, please refer to Appendix One.

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.

9. 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.

- Staff might need to take Personal Data off the school site for various reasons, for example because they are working from home or supervising a school trip. Appropriate safeguards must be put in place to protect personal data.
- When working away from the school you must only take the minimum amount of information with you.
- You must not work on documents containing Personal Data whilst travelling if there is a risk of unauthorised disclosure.
- If you need to take hard copy (i.e. paper) records off site, then you should make sure that they are kept secure.
- Critical School Personal Data should only be taken off the school site in hard copy when this is necessary.
- When working remotely you should not use public Wi-Fi.
- Documents containing Personal Data (including photographs and videos) should not be sent to or saved to personal devices save for the limited circumstances set out in the Guidance for staff on the use of photographs and videos by the school.
- If you use a personal device for school work which came with a default password, then this password should be changed immediately.
- You must take steps to ensure that others who use your device (for example, friends and family) cannot access anything school related on your device.

For further guidance, staff should refer to the school's Information Security Policy, which can be found in the staff handbook.

10. Processing of Financial / Credit Card Data

The School complies with the requirements of the PCI Data Security Standard ("PCI DSS"). Staff who are required to process credit card data must ensure that they are aware of and comply with the most up to date PCI DSS requirements. If you are unsure in this regard, please seek further guidance from the Finance Director. Other categories of financial information, including bank details and salary, or information commonly used in identity theft (such as national insurance numbers or passport details) may not be treated as legally sensitive but can have material impact on individuals and should be handled accordingly.

11. Audit

11.1 The school, through its DPO, regularly tests its data systems and processes in order to assess compliance. This is done through data audits which take place annually in order to review use of personal data.

12. Direct Marketing

The school is subject to certain rules and privacy laws when marketing. For example, a data subject's prior consent will be required for electronic direct marketing (for example, by email).

The school will explicitly offer individuals the opportunity to object to direct marketing and will do so in an intelligible format which is clear for the individual to understand. The school will promptly respond to any individual objection to direct marketing.

13. Transparency and Privacy Notices

The school will provide detailed, specific information to data subjects. This information will be provided through the school's privacy notices which are concise, transparent, intelligible, easily accessible and in clear and plain language so that a data subject can easily understand them. The school's privacy notices are tailored to suit the data subject and set out information about how the school uses their data.

Whenever we collect personal data directly from data subjects, including for human resources or employment purposes, we will provide the data subject with all the information required by the UK GDPR. This includes the identity of the DPO, the school's contact details, how and why we will use, process, disclose, protect, and retain personal data. This information will be provided within our privacy notices which are available on the school website and can be made available in hard copy, large print or other accessible format if required; such requests can be made to bursar@kcs.org.uk..

When personal data is collected indirectly (for example, from a third party or a publicly available source), where appropriate, we will provide the data subject with the above information as soon as possible after receiving the data via our privacy notices.

Notifications shall be in accordance with ICO guidance and where relevant, be written in a form understandable by those defined as "children" under the UK GDPR.

14. Privacy by Design

The school adopts a privacy by design approach to data protection to ensure that we adhere to data compliance and to implement technical and organisational measures in an effective manner.

Privacy by design is an approach that promotes privacy and data protection compliance from the start. To help us achieve this, the school takes into account the nature and purposes of the processing, any cost of implementation and any risks to rights and freedoms of data subjects when implementing data processes.

APPENDIX 1

SUBJECT ACCESS REQUESTS

1. Introduction

1.1. Under Data Protection Law, data subjects have a general right to find out whether the school holds or processes personal data about them, to access that data, and to be given supplementary information. This is known as the right of access or the right to make a data subject access request (SAR). The purpose of the right is to enable the individual to be aware of and verify the lawfulness of the processing of personal data that the school is undertaking.

1.2. This section provides guidance for staff members on how data subject access requests should be handled and for all individuals on how to make a SAR.

1.3. Failure to comply with the right of access under UK GDPR puts both staff and the school at potentially significant risk and so the school takes compliance with this policy very seriously.

1.4. A data subject has the right to be informed by the school of the following:

(a) Confirmation that their data is being processed;

(b) Access to their personal data;

(c) A description of the information that is being processed;

(d) The purpose for which the information is being processed;

(e) The recipients/class of recipients to whom that information is or may be disclosed;

(f) Details of the school's sources of information obtained;

(g) In relation to any personal data processed for the purposes of evaluating matters in relation to the data subject that has constituted or is likely to constitute the sole basis for any decision significantly affecting him or her, to be informed of the logic of the data controller's decision making. Such data may include, but is not limited to, performance at work, creditworthiness, reliability, and conduct; and

(h) Other supplementary information.

2. How to Recognise a Subject Access Request

A data subject access request is a request from an individual (or from someone acting with the authority of an individual, e.g. a solicitor or a parent making a request in relation to information relating to their child):

- for confirmation as to whether the school processes personal data about him or her and, if so
- for access to that personal data
- and/or certain other supplementary information

2.1. A valid SAR can be both in writing (by letter, email, WhatsApp text, social media) or verbally (e.g., during a telephone conversation or meeting). The request may refer to the UK GDPR and/or to 'data protection' and/or to 'personal data' but does not need to do so in order to be a valid request. For example, a letter which states 'please provide me with a copy of information that the school holds about me' would constitute a data subject access request and should be treated as such.

2.2. A data subject is generally only entitled to access their own personal data and not information relating to other people.

3. How to Make a Data Subject Access Request

3.1. Whilst there is no requirement to do so, we encourage any individuals who wish to make such a request to make the request in writing, detailing exactly the personal data being requested. This allows the school to easily recognise that you wish to make a data subject access request and the nature of your request. If the request is unclear/vague we may be required to clarify the scope of the request which may in turn delay the start of the time period for dealing with the request. A subject access request form is attached at Appendix 2 which you may find it helpful to use.

4. What to do When You Receive a Data Subject Access Request

All data subject access requests should be immediately directed to the bursar who will contact Judicium as DPO as appropriate in order to assist with the request and what is required. There are limited timescales within which the school must respond to a request and any delay could result in failing to meet those timescales, which could lead to enforcement action by the Information Commissioner's Office (ICO) and/or legal action by the affected individual. If ever in doubt, please refer the request to the bursar.

5. Acknowledging the Request

When receiving a SAR, the school shall acknowledge the request as soon as possible and inform the requester about the statutory deadline (of one calendar month) to respond to the request.

5.1. In addition to acknowledging the request, the school may ask for:

- proof of ID (if needed);
- further clarification about the requested information if it is not clear what information is required;
- if it is not clear where the information shall be sent, the school must clarify what address/email address to use when sending the requested information; and/or
- consent (if requesting third party data).

5.2. The school will work with their DPO as appropriate in order to create the acknowledgment.

6. Verifying the Identity of a Requester or Requesting Clarification of the Request

6.1. Before responding to a SAR, the school will take reasonable steps to verify the identity of the person making the request. In the case of current employees, this will usually be straightforward. The school is entitled to request additional information from a requester in order to verify whether the requester is in fact who they say they are. Where the school has reasonable doubts as to the identity of the individual making the request, evidence of identity may be established by production of a passport, driving license, a recent utility bill with current address, birth/marriage certificate, credit card or a mortgage statement.

6.2. If an individual is requesting a large amount of data the school may ask the requester for more information for the purpose of clarifying the request, but the requester shall never be asked why the request has been made. The school shall let the requestor know as soon as possible where more information is needed before responding to the request.

6.3. When it is necessary to verify the identity of the person making the request, the one calendar month period for responding begins when sufficient confirmation of identity is provided.

6.4. When it is necessary to request more information for the purpose of clarifying the request, the one calendar month period for responding pauses when further information is requested and does not restart until sufficient clarification is provided.

6.5. In both cases, the school will be unable to comply with the request if they do not receive the additional information.

7. Requests Made by Third Parties or on Behalf of Children

The school needs to be satisfied that the third party making the request is entitled to act on behalf of the individual, but it is the third party's responsibility to provide evidence of this entitlement. This might be a written authority to make the request, or it might be a more general power of attorney. The school may also require proof of identity in certain circumstances.

If the school is in any doubt or has any concerns as to providing the personal data of the data subject to the third party, then it should provide the information requested directly to the data subject. It is then a matter for the data subject to decide whether to share this information with any third party.

7.1. When requests are made on behalf of children, it is important to note that even if a child is too young to understand the implications of subject access rights, it is still the right of the child, rather than of anyone else such as a parent or guardian, to have access to the child's personal data. Before responding to a SAR for information held about a child, the school should consider whether the child is mature enough to understand their rights. If the school is confident that the child can understand their rights, then the school should usually respond directly to the child or seek their consent before releasing their information.

7.2. It shall be assessed if the child is able to understand (in broad terms) what it means to make a subject access request and how to interpret the information they receive as a result of doing so. When considering borderline cases, it should be taken into account, among other things:

- the child's level of maturity and their ability to make decisions like this;
- the nature of the personal data;
- any court orders relating to parental access or responsibility that may apply;
- any duty of confidence owed to the child or young person;
- any consequences of allowing those with parental responsibility access to the child's or young person's information. This is particularly important if there have been allegations of abuse or ill treatment;
- any detriment to the child or young person if individuals with parental responsibility cannot access this information; and
- any views the child or young person has on whether their parents should have access to information about them.

7.3. Generally, a person aged 12 years or over is presumed to be of sufficient age and maturity to be able to exercise their right of access, unless the contrary is shown. In relation to a child 12 years of age or older, then provided that the school is confident that they understand their rights and there is no reason to believe that the child does not have the capacity to make a request on their own behalf, the school will require the written authorisation of the child before responding to the requester or provide the personal data directly to the child.

7.4. The school may also refuse to provide information to parents if there are consequences of allowing access to the child's information – for example, if it is likely to cause detriment to the child.

8. Fee For Responding to a SAR

8.1. The school will usually deal with a SAR free of charge. Where a request is considered to be manifestly unfounded or excessive a fee to cover administrative costs may be requested. If a request is considered to be manifestly unfounded or unreasonable the school will inform the requester why this is considered to be the case and that the school will charge a fee for complying with the request.

8.2. A fee may also be requested in relation to repeat requests for copies of the same information. In these circumstances a reasonable fee will be charged taking into account the administrative costs of providing the information.

8.3. If a fee is requested, the period of responding begins when the fee has been received.

9. Time Period for Responding to a SAR

9.1. The school has one calendar month to respond to a SAR. This will run from the day that the request was received or from the day when any additional identification or other information requested is received, or payment of any required fee has been received.

9.2. The circumstances where the school is in any reasonable doubt as to the identity of the requester, this period will not commence unless and until sufficient information has been provided by the requester as to their identity and in the case of a third party requester, the written authorisation of the data subject has been received. Where the school may be required to get consent from a pupil, the time period will not start until consent is received.

9.3. The period for response may be extended by a further two calendar months in relation to complex requests. What constitutes a complex request will depend on the particular nature of the request. The DPO will be consulted as necessary in determining whether a request is sufficiently complex as to extend the response period. Where a request is considered to be sufficiently complex as to require an extension of the period for response, the school will need to notify the requester within one calendar month of receiving the request, together with reasons as to why this extension is considered necessary.

10. School Closure Periods

10.1. Outside of term time there are a limited number of staff on site. The school will endeavour to comply with requests as soon as possible and will keep in communication with you as far as possible. However, please provide your request during term times and not during/close to closure periods where possible.

11. Information to be Provided in Response to a Request

11.1. The individual is entitled to receive access to the personal data we process about him or her and the following information:

- the purpose for which we process the data;
- the recipients or categories of recipient to whom the personal data has been or will be disclosed, in particular where those recipients are in third countries or international organisations;
- where possible, the period for which it is envisaged the personal data will be stored, or, if not possible, the criteria used to determine that period;
- the fact that the individual has the right:
    - to request that the Company rectifies, erases, or restricts the processing of his or her personal data; or
    - to object to its processing;
    - to lodge a complaint with the ICO;

- where the personal data has not been collected from the individual to any information available regarding the source of the data.

11.2. The information should be provided in a way that is concise, transparent, easy to understand and easy to access using clear and plain language, with any technical terms, abbreviations or codes explained. The response shall be given in writing if the SAR was made in writing in a commonly used electronic format.

11.3. The information that the school is required to supply in response to a SAR must be supplied by reference to the data in question at the time the request was received. However, as the school has one month in which to respond the school is allowed to take into account any amendment or deletion made to the personal data between the time the request is received and the time the personal data is supplied if such amendment or deletion would have been made regardless of the receipt of the SAR.

11.4. Therefore, the school is allowed to carry out regular housekeeping activities even if this means deleting or amending personal data after the receipt of a SAR. The school is not allowed to amend or delete data to avoid supplying the data.

12. How to Locate Information

12.1. The personal data the school needs to provide in response to a data subject access request may be located in several of the electronic and manual filing systems. This is why it is important to identify at the outset the type of information requested so that the search can be focused.

12.2. Depending on the type of information requested, the school may need to search all or some of the following:

- electronic systems, e.g., databases, networked and non-networked computers, servers, customer records, human resources system, email data, back up data, CCTV;
- manual filing systems in which personal data is accessible according to specific criteria, e.g., chronologically ordered sets of manual records containing personal data;
- data systems held externally by our data processors;
- safeguarding systems (such as KIM/secure notes);
- MIS system (such as SchoolBase);
- occupational health records;
- pensions data;
- insurance benefit information.

12.3. The school should search these systems using the individual's name, initials, employee number or other personal identifier as a search determinant.

13. Protection of Third Parties - Exemptions to the Right of Subject Access

There are circumstances where information can be withheld pursuant to a SAR. These specific exemptions and requests should be considered on a case by case basis.

13.1. The school will consider whether it is possible to redact information so that this does not identify those third parties. If their data cannot be redacted (for example, after redaction it is still obvious who the data relates to) then the school does not have to disclose personal data to the extent that doing so would involve disclosing information relating to another individual (including information identifying the other individual as the source of information) who can be identified from the information unless:

- the other individual has consented to the disclosure; or
- it is reasonable to comply with the request without that individual's consent.

13.2. In determining whether it is reasonable to disclose the information without the individual's consent, all of the relevant circumstances will be taken into account, including:

- the type of information that they would disclose;
- any duty of confidentiality they owe to the other individual;
- any steps taken to seek consent from the other individual;
- whether the other individual is capable of giving consent; and
- any express refusal of consent by the other individual.

It needs to be decided whether it is appropriate to disclose the information in each case. This decision will involve balancing the data subject's right of access against the other individual's rights. If the other person consents to the school disclosing the information about them, then it would be unreasonable not to do so. However, if there is no such consent, the school must decide whether to disclose the information anyway. If there are any concerns in this regard, then the DPO will be consulted.

14. Other Exemptions to the Right of Subject Access

14.1. In certain circumstances the school may be exempt from providing some or all of the personal data requested. These exemptions are described below and should only be applied on a case-by-case basis after a careful consideration of all the facts.

14.2. *Crime detection and prevention:* The school does not have to disclose any personal data being processed for the purposes of preventing or detecting crime; apprehending or prosecuting offenders; or assessing or collecting any tax or duty.

14.3. *Confidential references:* The school does not have to disclose any confidential references given to third parties for the purpose of actual or prospective:

- education, training, or employment of the individual;
- appointment of the individual to any office; or
- provision by the individual of any service.

14.4. This exemption does not apply to confidential references that the school receives from third parties. However, in this situation, granting access to the reference may disclose the personal data of another individual (i.e., the person giving the reference), which means that the school must consider the rules regarding disclosure of third-party data set out above before disclosing the reference.

14.5. *Legal professional privilege:* The school does not have to disclose any personal data which is subject to legal professional privilege.

14.6. *Management forecasting:* The school does not have to disclose any personal data processed for the purposes of management forecasting or management planning to assist us in the conduct of any business or any other activity.

Negotiations: The school does not have to disclose any personal data consisting of records of intentions in relation to any negotiations with the individual where doing so would be likely to prejudice those negotiations.

15. Refusing to Respond to a Request

15.1. The school can refuse to comply with a request if the request is manifestly unfounded or excessive, taking into account whether the request is repetitive in nature.

15.2. If a request is found to be manifestly unfounded or excessive the school can:

- request a "reasonable fee" to deal with the request; or

- refuse to deal with the request.

15.3. In either case the school needs to justify the decision and inform the requestor about the decision.

15.4. The reasonable fee should be based on the administrative costs of complying with the request. If deciding to charge a fee the school should contact the individual promptly and inform them. The school does not need to comply with the request until the fee has been received.

16. Record Keeping

16.1. A record of all subject access requests shall be kept by the bursar. The record shall include the date the SAR was received, the name of the requester, what data the school sent to the requester and the date of the response.

APPENDIX 2

SUBJECT ACCESS REQUEST FORM

The Data Protection Act 2018 provides data subjects with a right to receive a copy of the data/information the school holds about them or to authorise someone to act on their behalf. Please complete the form at Appendix 1 if you wish to make a request for your data. Your request will normally be processed within one calendar month upon receipt of a fully completed form and proof of identity.

Proof of Identity: The school requires proof of your identity before it can disclose personal data. Proof of your identity should include a copy of a document such as your birth certificate, passport, driving licence, official letter addressed to you at your address e.g., bank statement, recent utilities bill or council tax bill. The document should include your name, date of birth and current address. If you have changed your name, please supply relevant documents evidencing the change.

Section 1: Please fill in the details of the data subject (i.e., the person whose data you are requesting). If you are not the data subject and you are applying on behalf of someone else, please fill in the details of the data subject below and not your own.

Title	
Surname/Family Name	
First Name(s)/ Forename	
Date of Birth	
Address	
Post Code	
Phone Number	
Email address	

I am enclosing the following copies as proof of identity (please tick the relevant box):
☐ Birth certificate
☐ Driving licence
☐ Passport
☐ An official letter to my address

Personal Information

If you only want to know what information is held in specific records, please indicate in the box below. Please tell us if you know in which capacity the information is being held, together with any names or dates you may have. If you do not know exact dates, please give the year(s) that you think may be relevant.

Details:

Employment records:

If you are, or have been employed by the school and are seeking personal information in relation to your employment please provide details of your staff number, unit, team, dates of employment etc.

Details:

Section 2

Please complete this section of the form with your details if you are acting on behalf of someone else (i.e., the data subject).

If you are NOT the data subject, but an agent appointed on their behalf, you will need to provide evidence of your identity as well as that of the data subject and proof of your right to act on their behalf.

Title	
Surname/ Family Name	
First Name(s)/Forenames	
Date of Birth	
Address	
Post Code	
Phone Number	

I am enclosing the following copies as proof of identity (please tick the relevant box):

☐ Birth certificate

☐ Driving licence

☐ Passport

☐ An official letter to my address

What is your relationship to the data subject? (e.g., parent, carer, legal representative)

I am enclosing the following copy as proof of legal authorisation to act on behalf of the data subject:

☐ Letter of authority

☐ Lasting or Enduring Power of Attorney

☐ Evidence of parental responsibility

☐ Other (give details):

Section 3

Please describe as detailed as possible what data you request access to (e.g., time period, categories of data, information relating to a specific case, paper records, electronic records).

I wish to:

☐ Receive the information by post*

☐ Receive the information by email

☐ Collect the information in person

☐ View a copy of the information only

☐ Go through the information with a member of staff

*Please be aware that if you wish us to post the information to you, we will take every care to ensure that it is addressed correctly. However, we cannot be held liable if the information is lost in the post or incorrectly delivered or opened by someone else in your household. Loss or incorrect delivery may cause you embarrassment or harm if the information is 'sensitive'.

Please send your completed form and proof of identity by email to: bursar@kcs.org.uk