

The General Data Protection Regulation provides the following rights for individuals:

1. The right to be informed
  - Individuals have the right to be informed about the collection and use of their personal data.
  - We will provide individuals with information including: our purpose for processing their personal data, our retention period for that personal data, and who it will be shared with.
  - This information is shared when we gather consent of through our Privacy Notices – available on the school website
2. The right of access
  - Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them.
  - Subject access requests must be submitted in writing, either by letter, email or fax to the Data Protection Officer (DPO). They should include:
    - Name of individual
    - Correspondence address
    - Contact number and email address
    - Details of the information requested
  - To make a Subject Access Request, contact
    - Mr James Robinson – SESSET Data Protection Officer, robinson.james@ashcombe.surrey.sch.uk, or at The Ashcombe School, Ashcombe Road, Dorking, Surrey, RH41LY.
    - Mr Paul Thompson – Data Protection Lead, PWorrallThompson@therfield.surrey.sch.uk, or at Therfield School, Dilston Road, Leatherhead, SURREY, KT22 7NZ.
    - Mr Ben Stafford - Data Protection Lead, sd@warwick.surrey.sch.uk, or at Noke Drive, Redhill, RH1 4AD.
3. The right to rectification
  - The GDPR includes a right for individuals to have inaccurate personal data rectified, or completed if it is incomplete. We will routinely contact parents to confirm the data we hold is up to date.
  - If you become aware of further need for change, please email our main school email address and state "Request for data rectification".
  - **Consent**
    - Where required we will seek positive, affirmative consent in advance.
    - We will regularly reconfirm consent.
    - If, between these times, you wish to withdraw consent please contact the main school email address and state "Request to withdraw consent".
4. The right to erasure
  - The GDPR introduces a right for individuals to have personal data erased. The right to erasure is also known as 'the right to be forgotten'.
  - Individuals can make a request for erasure verbally or in writing however, the right is not absolute and only applies in certain limited circumstances.
  - If you believe this might apply and you wish to request erasure of data, please email our main school email address and state "Request for data erasure".
5. The right to restrict processing
  - Individuals have the right to request the restriction or suppression of their personal data.
  - This is not an absolute right and only applies in certain circumstances.
  - If you believe this might apply and you wish to request erasure of data, please email our main school email address and state "Request for restriction of processing".
6. The right to data portability
  - Data is transferred from and to any other schools through Common Transfer Files.
7. The right to object
  - Individuals have the right to object to:
    - processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
    - processing for purposes of scientific/historical research and statistics.
  - Requests will be treated on grounds relating to his or her particular situation.
8. Rights in relation to automated decision making and profiling.
  - We don't make automated decisions without human involvement.

### **Notification of data security breach**

- In the unlikely event you discover a data security breach we will prioritise this as an urgent issue.
- If you believe you have discovered data security breach, please email our main school email address and state "Urgent – Data security breach notification" in the email subject.
- This will be reported to our Data Protection Team and logged at an appropriate level.

- The GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority. We will do this within 72 hours of becoming aware of the breach, where feasible.
- If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, we will also inform those individuals without undue delay.