

DATA PROTECTION POLICY

This policy will be reviewed every year for the next two years to ensure any further guidance issued by the ICO is reflected within the policy.

1. Aims

Our School aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Legislation and guidance

This policy meets the requirements of the GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.

It meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data.

It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

3. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: <ul style="list-style-type: none"> • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: <ul style="list-style-type: none"> • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating,

	erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. The data controller

Our School processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller.

The school is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

5. Roles and responsibilities

This policy applies to **all staff** employed by our school, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

5.1 Governing Body

The Governors have overall responsibility for ensuring that our school complies with all relevant data protection obligations.

5.2 Data protection officer

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

They will provide an annual report of their activities directly to the Governing Body and, where relevant, report to the Body their advice and recommendations on school data protection issues.

The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO.

Full details of the DPO's responsibilities are set out in their job description.

Our DPO is **(to be appointed)** and is contactable via dpo@twggs.kent.sch.uk

5.3 Head Teacher

The Head Teacher and Bursar act as the representative of the data controller on a day-to-day basis.

5.4 All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address
- Contacting the DPO in the following circumstances:
 - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
 - If they have any concerns that this policy is not being followed
 - If they are unsure whether or not they have a lawful basis to use personal data in a particular way

- If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
- If there has been a data breach
- Whenever they are engaging in a new activity that may affect the privacy rights of individuals
- If they need help with any contracts or sharing personal data with third parties

6. Data protection principles

The GDPR is based on data protection principles that our school must comply with.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

This policy sets out how the school aims to comply with these principles.

7. Collecting personal data

7.1 Lawfulness, fairness and transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract
- The data needs to be processed so that the school can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life
- The data needs to be processed so that the school, as a public authority, can perform a task **in the public interest**, and carry out its official functions
- The data needs to be processed for the **legitimate interests** of the school or a third party (provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

Secondary schools

If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent where the pupil is under 13 (except for online counselling and preventive services).

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

7.2 Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to process personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the school's record retention schedule/records management policy.

8. Sharing personal data

We will not normally share personal data with anyone else, but may do so where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff/ governors/ individuals working on our behalf at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:

- Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
- Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
- Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

9. Subject access requests and other rights of individuals

9.1 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Subject access requests must be submitted in writing, either by letter or email to the DPO. They should include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If staff receive a subject access request they must immediately forward it to the DPO [or email dpo@twggs.kent.sch.uk](mailto:dpo@twggs.kent.sch.uk)

9.2 Children and subject access requests

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

Secondary schools

Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our school may not be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

9.3 Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made

- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

9.4 Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

10. Parental requests to see the educational record

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request.

11. Photographs and videos

As part of our school activities, we may take photographs and record images of individuals within our school.

Secondary schools

We will obtain written consent from parents/carers, or pupils aged 17 and over, for photographs and videos to be taken of pupils for communication, marketing and promotional materials.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil. Where we don't need parental consent, we will clearly explain to the pupil how the photograph and/or video will be used.

Uses may include:

- Within the school on notice boards and in school magazines, brochures, newsletters, etc.
- Outside of the school by external agencies such as the school photographer, newspapers, campaigns
- Online on our school websites or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

See our Safeguarding Policy for more information on our use of photographs and videos.

12. Data protection by design and default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing data protection impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
 - For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
 - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

13. Data security and storage of records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Where personal information needs to be taken off site other than for trips and visits, staff must sign it in and out from the school office. Staff accompanying trips taken with them a pack of information, authorised by the Educational Visits Coordinator/ Assistant Headteacher, as outlined in the Educational Visits Policy. Senior members of staff with a requirement to take personal information off site regularly follow an alternative agreed appropriate system.
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our online safety policy/ICT policy/acceptable use agreement/policy on acceptable use.)
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

14. Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

15. Personal data breaches

The school will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure set out in Appendix 1. When appropriate, we will report the data breach to the ICO within 72 hours of becoming aware of the breach. Staff, governors and data processors must be aware that their knowledge or suspicion of a breach marks the beginning of this time frame, thus time is of the essence in following the requirements of Appendix 1.

Such breaches in a school context may include, but are not limited to:

- A non-anonymised dataset being published on the school website which shows the exam results of pupils eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about pupils

16. Training

All staff and governors are provided with data protection training as part of their induction process.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

17. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated if necessary when the Data Protection Bill receives royal assent and becomes law (as the Data Protection Act 2018) – if any changes are made to the bill that affect our school's practice. Otherwise, or from then on, this policy will be reviewed **every year**.

18. Links with other policies

This data protection policy is linked to our:

- Freedom of information publication scheme
- Online Safety Policy
- Acceptable Use of ICT statement
- Child Protection (Safeguarding) Policy
- Records Management & Retention Guidelines Policy
- Whistleblowing Policy
- Educational Visits Policy
- Image Use Policy

Appendix 1: Personal data breach procedure

This procedure is based on [guidance on personal data breaches](#) produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member, governor or data processor must immediately notify the DPO
- The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
 - Lost
 - Stolen
 - Destroyed
 - Altered
 - Disclosed or made available where it should not have been
 - Made available to unauthorised people
- The DPO will alert the Headteacher and the Chair of Governors
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
 - Loss of control over their data
 - Discrimination
 - Identify theft or fraud
 - Financial loss
 - Unauthorised reversal of pseudonymisation (for example, key-coding)
 - Damage to reputation
 - Loss of confidentiality
 - Any other significant economic or social disadvantage to the individual(s) concerned

If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.

- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on GDPRiS Software
- Where the ICO must be notified, the DPO will do this via the ['report a breach' page of the ICO website](#) within 72 hours of becoming aware of the breach. As required, the DPO will set out:
 - A description of the nature of the personal data breach including, where possible:
 - The categories and approximate number of individuals concerned
 - The categories and approximate number of personal data records concerned
 - The name and contact details of the DPO
 - A description of the likely consequences of the personal data breach
 - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned
- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
 - The name and contact details of the DPO
 - A description of the likely consequences of the personal data breach
 - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned

- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
 - Facts and cause
 - Effects
 - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

Records of all breaches will be stored on GDPRiS software.

The DPO and Headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

Actions to minimise the impact of data breaches

We will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to recall it
- In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way
- The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request
- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted

Other types of breach that might be considered could include:

- Details of pupil premium interventions for named children being published on the school website
- Non-anonymised pupil exam results or staff pay information being shared with governors
- A school laptop containing non-encrypted sensitive personal data being stolen or hacked
- The school's cashless payment provider being hacked and parents' financial details stolen

Appendix 2: Consents forms - Parents (Year 7 and new entrants) and Pupils (Year 8 and U6th)

New Year 7 - Parental Consent – please complete and return one copy to TWGGS

Pupil name:

Form:

There are a number of aspects relating to school life at TWGGS, for which we need to seek your consent, under the requirements of the General Data Protection Regulation (GDPR).

- **School photographers:** an external company (currently Van Cols) takes photographs of individual pupils, forms, year groups and the whole school throughout pupils' time at TWGGS. These photographs are offered to parents for sale, and the individual photographs in Years 7, 9 and L6th are held electronically on the school information management system (SIMS) to enable identification of pupils. Whole school photographs and year group photographs of Years 11 and U6th are put on display in the school building.
- **Harrison Catering Service Ltd and sQuid (on-line payment company used by Harrisons for payment of school lunches):** the names and forms of any pupils joining the school are passed to Harrisons for the purpose of setting up/ maintaining lunch accounts. Photos are taken for identification attached to the canteen card. Harrisons also hold details of dietary requirements and the names of any pupil in receipt of Free School Meals. Harrison Catering initially provide to sQuid the names of any pupils new to the school to enable a sQuid account registration number to be generated – this is then provided to parents/carers for them then to register directly with sQuid.
- **ParentPay:** school provides names of pupils; parents register in order to pay for school trips and activities online.
- **Edmodo:** all pupils in Years 7-9 study Computing, and those in Years 10 and 11 who opt for GCSE Computing, have an Edmodo account with a username and password. Pupils provide their names when setting up the account; email address is optional and pupils are told by their teacher not to enter one. All work produced in lessons is attached along with tests and marks/grades. Each year, groups are archived and deleted a year later which removes all class data/grades/marks. Although groups are deleted, the Edmodo accounts remain active; school cannot delete these, although pupils are able to. The privacy notice may be viewed here: <https://go.edmodo.com/privacy/>
- **Vocab Express:** the school subscribes to Vocab Express to aid pupils' language learning across Spanish, German and French, in particular as a dynamic and highly effective way of learning vocabulary, and enabling teachers to monitor and track progress. Pupils have personalised log in details with passwords.
- **Fronter:** this is the online learning platform used by the school, on which a range of learning resources are placed by teachers. Pupils have individual log in details and set their own passwords.
- **Fast Tomato:** this is an online careers resource, used in Year 9; pupils put in name and date of birth to register, then have individual log in details and set their own passwords; an email address is optional and pupils are told not to enter one.
- **Project Q:** L6th pupils studying the Extended Project Qualification register themselves to use this online system.
- TWGGS publishes destinations information (a pupil's name, higher education or career destination and course/ job role) on a Destinations Board in the school reception area. This is also published in the School Record, given to each pupil and parent attending Speech Day (ex-Year 11 and U6th). The School Record also includes all these pupils' names, any prizes won and an identifier for grades 7, 8 and 9 at GCSE, A*/A at A Level.

Please sign below to indicate your consent to the above, deleting any areas where consent is denied. You may withdraw your consent at any time.

Parent/ carer name:

Signature:

Parent/ carer name:

Signature:

Please note, in line with GDPR requirements, pupils' consent will also be sought at the beginning of Year 8 & U6th.

Day trips/ activities

In order to save you and the school the need to complete an indemnity form each time your child goes out of school, please complete and return the following. This will cover all trips of up to one day's duration - particularly such things as sports' fixtures, theatre and museum trips, throughout their school career. For residential visits, any hazardous activities, or those abroad (even if only a day trip), you will be required to complete a separate form.

I consent to my child taking part in school trips of up to a day's duration, (e.g. sports fixtures, theatre and museum outings). I understand that while the school staff in charge of the party will take all reasonable care of the children, they cannot necessarily be held responsible for any loss, damage or injury suffered by my child which may occur as a result of the trip. Should the need arise I agree to the person in charge of the party giving consent on my behalf for an anaesthetic to be administered or for any other urgent medical treatment to be given.

The date of my child's last tetanus injection was:

Signatures of ALL persons with Legal Responsibility

Signed:

Signed:

Child's name:

Form:

NB Please note, all persons with legal responsibility must sign, even parents/carers living apart from the child

Pupil consent form – Year 8

Pupil name:

Form:

There are a number of aspects relating to school life at TWGGS, for which we need to seek your consent, under the requirements of the General Data Protection Regulation (GDPR). Your parents also have the opportunity to give their agreement (or otherwise).

- **School photographers:** an external company (currently Van Cols) takes photographs of individual pupils, forms, year groups and the whole school throughout pupils' time at TWGGS. These photographs are offered to parents for sale, and the individual photographs in Years 7, 9 and L6th are held electronically on the school information management system (SIMS) to enable identification of pupils. Whole school photographs and year group photographs of Years 11 and U6th are put on display in the school building.
- **Harrison Catering Service Ltd and sQuid (on-line payment company used by Harrison Catering for payment of school lunches):** the names and forms of any pupils joining the school are passed to Harrisons for the purpose of setting up/ maintaining lunch accounts. Photos are taken for identification attached to the canteen card. Harrisons also hold details of dietary requirements and the names of any pupil in receipt of Free School Meals. Harrison Catering initially provide to sQuid the names of any pupils new to the school to enable a sQuid account registration number to be generated – this is then provided to parents/carers for them then to register directly with sQuid.
- **ParentPay:** school provides names of pupils; parents register in order to pay for school trips and activities online.
- **Edmodo:** all pupils in Years 7-9 study Computing, and those in Years 10 and 11 who opt for GCSE Computing, have an Edmodo account with a username and password. Pupils provide their names when setting up the account; email address is optional and pupils are told by their teacher not to enter one. All work produced in lessons is attached along with tests and marks/grades. Each year, groups are archived and deleted a year later which removes all class data/grades/marks. Although groups are deleted, the Edmodo accounts remain active; school cannot delete these, although pupils are able to. The privacy notice may be viewed here: <https://go.edmodo.com/privacy/>
- **Vocab Express:** the school subscribes to Vocab Express to aid pupils' language learning across Spanish, German and French, in particular as a dynamic and highly effective way of learning vocabulary, and enabling teachers to monitor and track progress. Pupils have personalised log in details with passwords.
- **Fronter:** this is the online learning platform used by the school, on which a range of learning resources are placed by teachers. Pupils have individual log in details and set their own passwords.
- **Fast Tomato:** this is an online careers resource, used in Year 9; pupils put in name and date of birth to register, then have individual log in details and set their own passwords; an email address is optional and pupils are told not to enter one.
- **Project Q:** L6th pupils studying the Extended Project Qualification register themselves to use this online system.
- TWGGS publishes destinations information (a pupil's name, higher education or career destination and course/ job role) on a Destinations Board in the school reception area. This is also published in the School Record, given to each pupil and parent attending Speech Day (ex-Year 11 and U6th). The School Record also includes all these pupils' names, any prizes won and an identifier for grades 7, 8 and 9 at GCSE, A*/A at A Level.

Please sign below to indicate your consent to the above, deleting any areas where you do not give your consent. You may withdraw your consent at any time.

Pupil signature:

Date:

Pupil consent form – Sixth Form

Pupil name:

Form:

There are a number of aspects relating to school life at TWGGS, for which we need to seek your consent, under the requirements of the General Data Protection Regulation (GDPR). Your parents also have the opportunity to give their agreement (or otherwise), however, as you will reach the age of 18 during this academic year, your individual consent is obviously important to us.

- **School photographers:** an external company (currently Van Cols) takes photographs of individual pupils, forms, year groups and the whole school throughout pupils' time at TWGGS. These photographs are offered to parents for sale, and the individual photographs in Years 7, 9 and L6th are held electronically on the school information management system (SIMS) to enable identification of pupils. Whole school photographs and year group photographs of Years 11 and U6th are put on display in the school building.
- **Harrison Catering Service Ltd and sQuid (on-line payment company used by Harrison Catering for payment of school lunches):** the names and forms of any pupils joining the school are passed to Harrisons for the purpose of setting up/ maintaining lunch accounts. Photos are taken for identification attached to the canteen card. Harrisons also hold details of dietary requirements and the names of any pupil in receipt of Free School Meals. Harrison Catering initially provide to sQuid the names of any pupils new to the school to enable a sQuid account registration number to be generated – this is then provided to parents/carers for them then to register directly with sQuid.
- **ParentPay:** school provides names of pupils; parents register in order to pay for school trips and activities online.
- **Edmodo:** all pupils in Years 7-9 study Computing, and those in Years 10 and 11 who opt for GCSE Computing, have an Edmodo account with a username and password. Pupils provide their names when setting up the account; email address is optional and pupils are told by their teacher not to enter one. All work produced in lessons is attached along with tests and marks/grades. Each year, groups are archived and deleted a year later which removes all class data/grades/marks. Although groups are deleted, the Edmodo accounts remain active; school cannot delete these, although pupils are able to. The privacy notice may be viewed here: <https://go.edmodo.com/privacy/> Whilst you no longer use this account in school and therefore we are not seeking consent, you may wish to delete it.
- **Vocab Express:** the school subscribes to Vocab Express to aid pupils' language learning across Spanish, German and French, in particular as a dynamic and highly effective way of learning vocabulary, and enabling teachers to monitor and track progress. Pupils have personalised log in details with passwords.
- **Fronter:** this is the online learning platform used by the school, on which a range of learning resources are placed by teachers. Pupils have individual log in details and set their own passwords.
- **Project Q:** L6th pupils studying the Extended Project Qualification register themselves to use this online system.
- TWGGS publishes destinations information (a pupil's name, higher education or career destination and course/ job role) on a Destinations Board in the school reception area. This is also published in the School Record, given to each pupil and parent attending Speech Day (ex-Year 11 and U6th). The School Record also includes all these pupils' names, any prizes won and an identifier for grades 8 and 9 at GCSE, A*/A at A Level.

Please sign below to indicate your consent to the above, deleting any areas where you do not give your consent. You may withdraw your consent at any time.

Pupil signature:

Date:

GDPR – Sports Consent Form - Parents

Dear Parent/ Carer,

GDPR guidelines require schools to seek informed consent where personal information is shared. We therefore require consent for entering all sports fixtures and competitions.

If your child is selected to perform in any of the following sports teams for fixtures or tournaments, their personal details, name, date of birth and in some cases Unique Pupil Number (UPN*), will be shared with the following organisations:

- Netball – England Netball and Kent Netball Association
- Hockey – England Hockey Association and Kent Hockey Association
- Sports Hall Athletics – Kent School Games
- Athletics – Kent School Games
- Tag Rugby – Sevenoaks Rugby, Kent Schools Rugby
- Trampolining – British Gymnastics and Kent Schools Trampolining and Kent School Games
- Gymnastics - British Gymnastics and South East Region Schools Gymnastics
- Tennis – Lawn Tennis Association and Kent Tennis
- Cricket – England Cricket Board and Kent Schools' Cricket Association
- Swimming- Kent Schools' Swimming Association
- Football – West Kent Schools' Football Association
- Equestrian – National Schools' Equestrian Association
- Skiing - English Schools' Ski Association

**The UPN is a number allocated nationally to all pupils as an identifier.*

Please sign and date below, and return this letter, giving consent to personal information being shared with the above named organisations. Delete any organisations where you do not give consent. Please note that the pupil would not then be able to represent the school in this sport, if selected. Your consent may be withdrawn at any time, by notifying the school in writing.

Yours faithfully,

Curriculum Leader PE

Pupil name:

Form:

I consent to my child being entered into sports fixtures and tournaments and therefore to relevant personal information being shared with the organisations stated above.

Signed: _____

Date: _____

GDPR – Sports Consent Form – Pupils Year 8 and above

Dear Pupil,

GDPR guidelines require schools to seek informed consent where personal information is shared. We therefore require consent for entering all sports fixtures and competitions.

If you are selected to perform in any of the following sports teams for fixtures or tournaments, your personal details, name, date of birth and in some cases Unique Pupil Number (UPN*), will be shared with the following organisations:

- Netball – England Netball and Kent Netball Association
- Hockey – England Hockey Association and Kent Hockey Association
- Sports Hall Athletics – Kent School Games
- Athletics – Kent School Games
- Tag Rugby – Sevenoaks Rugby, Kent Schools Rugby
- Trampolining – British Gymnastics and Kent Schools Trampolining and Kent School Games
- Gymnastics - British Gymnastics and South East Region Schools Gymnastics
- Tennis – Lawn Tennis Association and Kent Tennis
- Cricket – England Cricket Board and Kent Schools' Cricket Association
- Swimming- Kent Schools' Swimming Association
- Football – West Kent Schools' Football Association
- Equestrian – National Schools' Equestrian Association
- Skiing - English Schools' Ski Association

**The UPN is a number allocated nationally to all pupils as an identifier.*

Please sign and date below, and return this letter, giving consent to personal information being shared with the above named organisations. Delete any organisations where you do not give consent. Please note that you would not then be able to represent the school in this sport, if selected. Your consent may be withdrawn at any time, by notifying the school in writing.

Yours faithfully,

Curriculum Leader PE

Pupil name:

Form:

I consent to being entered into sports fixtures and tournaments and therefore to relevant personal information being shared with the organisations stated above.

Signed: _____

Date: _____

Appendix 2: Privacy Notice for Tunbridge Wells Girls' Grammar School (TWGGS) – Pupils and Parents

This notice explains what personal data (information) we hold about you, how we collect, how we use and may share information about you. We are required to give you this information under data protection law.

Who are we?

TWGGS collects, uses and is responsible for certain personal information about you. When we do so we are regulated under the General Data Protection Regulation which applies across the European Union (including in the United Kingdom) and we are responsible as 'controller' of that personal information for the purposes of those laws.

The personal information we collect and use

Information collected by us

In the course of providing education we collect the following personal information when you provide it to us:

- Personal information (such as name, unique pupil number, contact details, language, nationality, country of birth, and free school meal eligibility)
- Special category characteristics
 - Ethnicity
 - Special educational needs and disability (SEND) information
 - Relevant medical information
- Safeguarding information (such a court orders and professional involvement)
- Attendance information (such as sessions attended, number of absences and absence reasons)
- National curriculum assessment and public examination results
- Internal assessment results
- Careers details
- Destinations after leaving TWGGS

We also obtain personal information from other sources as follows:

- Personal information, special category information, assessment results and SEN information from schools that you previously attended
- For pupils enrolling for post 14 qualifications, the Learning Records Service will give us the unique learner number (ULN) and may also give us details about your learning or qualifications.
- Service support and involvement information from KCC teams working to improve outcomes for children and young people (such as SEND, Early Help, Free School Meals, Admissions)

How we use your personal information

We use your personal information to:

- Support pupil learning
- Monitor and report on pupil progress
- Moderate teacher assessment judgements
- Provide appropriate pastoral care and support services
- Assess the quality of our services
- Process any complaints
- Comply with the law regarding data sharing
- Support you to decide what to do after you leave school
- Support or improve educational provision
- Ensure no children are missing education
- Support children at risk of permanent exclusion
- Support the secondary and in-year admissions process
- Safeguard children and young people
- The prevention and detection of crime
- Improve the education and services we provide

Individual examination results for pupils, who have achieved high grades or made excellent progress, are published in the local press and media and also on TWGGS website.

How long your personal data will be kept

We will hold your personal information securely and retain it from the child/young person's date of birth until they reach the age of 25, after which the information is archived or securely destroyed.

Personal data will be retained by the school in accordance with the Data Retention guidelines in the Information Management Toolkit for Schools (IRMS). Electronic and paper student records (excluding contact information) will be held until a student reaches the age of 25 in accordance with the Limitation Act 1980 (Section 2) (or age of 30 if the student was statemented or had an EHCP in order to protect against a “failure to provide a sufficient education” case.)

After this time the school will maintain a school roll detailing the names of pupils who have been to the school with their dates of birth and recording between which dates they attended TWGGS. This will enable ex-pupils to allow potential employers to check this information.

Reasons we can collect and use your personal information

We collect and use pupil information under section 537A of the Education Act 1996, section 83 of the Children Act 1989, and to carry out tasks in the public interest. If we need to collect special category (sensitive) personal information, we rely upon reasons of substantial public interest (equality of opportunity or treatment). We process personal data because it is necessary in order to comply with the school’s legal obligations and to enable it to perform tasks carried out in the public interest. We are required by The Education (Pupil Information) (England) Regulations 2005 to maintain a Pupil’s Educational Record.

If there is processing or sharing that relies on your consent, we will make this clear to you and ensure we seek your consent.

Photographs

As part of our recording of events, celebrations and achievements, TWGGS may wish to take photographs of activities that involve your child. The photographs may be used for displays, publications and website(s) by the school, Local Authority (LA), local newspapers and other approved partners such as charities we support and local businesses working in partnership with the school on such things as enterprise challenges.

Photography and/or filming will only take place with the permission of the Headteacher and under appropriate supervision. When filming or photography is carried out by the news media, children may be named, but home addresses will not be disclosed. Images that might cause embarrassment or distress will not be used, including images associated with material on sensitive issues.

When a pupil joins the school, parents are asked to indicate whether they are happy for photographs of their child to be used on school, local authority or press websites; inside school only; or do not want any photographs of their child to be published at all.

All pupils have a photograph taken and stored internally in order to identify them for safeguarding purposes.

Who we share your personal information with

- Department for Education (DfE) (statutory for school funding and educational attainment policy and monitoring) and other government agencies and local authorities as required (e.g. to resolve funding queries)
- Kent County Council teams working to improve outcomes for children and young people
- Commissioned providers of local authority services (such as education services)
- Schools or colleges that you attend after leaving us
- Local forums with schools and KCC representatives which support in-year fair access processes and support managed moves between schools
- Local multi-agency forums which provide SEND advice, support and guidance (such as Local Inclusion Forum Team (LIFT))
- Partner organisations signed up to the Kent & Medway Information Sharing Agreement, where necessary, which may include Police, school nurses, doctors and mental health workers and Kent Community Health NHS Foundation Trust
- Local Authority – Social Services - in order to comply with our statutory safeguarding duties we are required, by law, to pass certain information about our pupils to local authorities. Information will only be shared where it is fair and lawful to do so.
- Schools in our local collaboration, to enable the moderation of pupil assessment outcomes, to support collaborative working through joint analysis, and ensure children continue to receive appropriate education provision
- Organisations which produce information for pupil target-setting and tracking
 - GL Assessment, for Cognitive Ability Tests (These provide a measure of cognitive reasoning ability, without reference to curriculum-based material and regardless of previous achievements or first language.)
 - FFT Aspire (provides estimates and data to support effective target-setting and self-evaluation.)
 - ALPS (provides value-added, analytical reports of individuals and groups at A Level)
- KCC has to share information with external moderators (teachers with recent relevant experience) of end of key stage assessments, to meet statutory requirements from the Standards & Testing Agency (STA)

- Exam Boards – pupils’ exams-related data may be shared with awarding bodies, the Joint Council for Qualifications, the Department for Education and Local Authority; this data may relate to exam entries, access arrangements, the conduct of exams and non-examination assessments, special consideration requests and exam results/post-results/certificate information.
- Third-party providers of information services (such as student apps) where consent has been given
- Contracted providers of services (such as school photographers, Parent Mail and catering providers) where consent has been given
- Harrison Catering Services Ltd and sQuid (on-line payment company used by Harrison Catering for payment of school lunches) – Harrison Catering is contractually engaged to operate catering within school. The names and forms of any pupils joining the school are passed to Harrison’s for the purpose of setting up/ maintaining lunch accounts. Harrison Catering also hold details of the names of any pupil in receipt of Free School Meals. Harrison Catering initially provide to sQuid the names of any pupils new to the school to enable a sQuid account registration number to be generated – this is then provided to parents/carers for them then to register directly with sQuid

We will share personal information with law enforcement or other authorities if required by applicable law.

We are required to share information about our pupils with KCC and the Department for Education (DfE) under section 3 of The Education (Information About Individual Pupils) (England) Regulations 2013.

Aged 14+ qualifications

For pupils enrolling for post-14 qualifications, the Learning Records Service will give us a pupil’s unique learner number (ULN) and may also give us details about the pupil’s learning or qualifications

Our pupils in Year 11

We also provide additional pupil information to KCC to fulfil their responsibilities in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996:

- Intended destinations of pupils in Year 11 moving into Year 12
- Course offers for pupils in Year 11 moving into Year 12 (September Guarantee)
- Information for Kent Choices4U (careers advice and course application website)

Our pupils aged 16+

We will share information about pupils aged 16+ with our local authority as they have responsibilities in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996.

KCC has a legal responsibility to track all young people up to the age of 19 (and young adults with learning difficulties or disabilities up to the age of 25). The purpose of collecting this information is to assist the planning of education and training for young people and the support services they require. KCC will inform us of your current activity once you have left the school. This is in relation to education, training, employment with training you may be undertaking and whether you are NEET (not in Education, Employment or Training). Some of this information is then shared with the DfE who use the information to plan at a national level.

This information enables KCC to provide and arrange:

- post-16 education and training provision
- youth support services
- careers advice and guidance

The National Pupil Database (NPD)

The NPD is owned and managed by the DfE and contains information about pupils in schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the DfE. It is held in electronic format for statistical purposes. This information is securely collected from a range of sources including schools, local authorities and awarding bodies.

We are required by law, to provide information about our pupils to the DfE as part of statutory data collections such as the school census and early years’ census. Some of this information is then stored in the NPD. The law that allows this is the Education (Information About Individual Pupils) (England) Regulations 2013.

The DfE may share information about our pupils from the NPD with third parties who promote the education or well-being of children in England by:

- conducting research or analysis
- producing statistics

- providing information, advice or guidance

The DfE has robust processes in place to ensure the confidentiality of our data is maintained and there are stringent controls in place regarding access and use of the data. Decisions on whether DfE releases data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data
- the purpose for which it is required
- the level and sensitivity of data requested: and
- the arrangements in place to store and handle the data

To be granted access to pupil information, organisations must comply with strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

Your Rights

Under the GDPR you have rights which you can exercise free of charge which allow you to:

- Know what we are doing with your information and why we are doing it
- Ask to see what information we hold about you (Subject Access Requests)
- Ask us to correct any mistakes in the information we hold about you
- Object to direct marketing
- Make a complaint to the Information Commissioners Office
- Withdraw consent (if applicable)

Depending on our reason for using your information you may also be entitled to:

- Ask us to delete information we hold about you
- Have your information transferred electronically to yourself or to another organisation
- Object to decisions being made that significantly affect you
- Object to how we are using your information
- Stop us using your information in certain ways

We will always seek to comply with your request however we may be required to hold or use your information to comply with legal duties. Please note: your request may delay or prevent us delivering a service to you.

For further information about your rights, including the circumstances in which they apply, see the guidance from the UK Information Commissioners Office (ICO) on individuals' rights under the General Data Protection Regulation.

If you would like to exercise a right, please contact the Data Protection Officer via the school, either in writing, or on dpo@twggs.kent.sch.uk

Keeping your personal information secure

We have appropriate security measures in place to prevent personal information from being accidentally lost, or used or accessed in an unauthorised way. We limit access to your personal information to those who have a genuine business need to know it.

Those processing your information will do so only in an authorised manner and are subject to a duty of confidentiality.

We also have procedures in place to deal with any suspected data security breach. We will notify you and any applicable regulator of a suspected data security breach where we are legally required to do so.

Who to Contact and Where to go for Further Information

Please contact the Data Protection Officer via the school, either in writing, or on dpo@twggs.kent.sch.uk to exercise any of your rights, or if you have a complaint about why your information has been collected, how it has been used or how long we have kept it for.

If you would like to get a copy of the information about you that KCC shares with the DfE or post-16 providers or how they use your information, please contact the Information Resilience and Transparency Team at data.protection@kent.gov.uk.

For more information about services for children and young people, please go to: <http://www.kent.gov.uk/education-and-children> or the KCC website at www.kent.gov.uk

The General Data Protection Regulation also gives you right to lodge a complaint with a supervisory authority. The supervisory authority in the UK is the Information Commissioner who may be contacted at <https://ico.org.uk/concerns> or telephone 03031 231113.

For further information visit <https://www.kent.gov.uk/about-the-council/about-the-website/privacy-statement>

For further information about how the Department for Education uses your information:

To find out more about the pupil information we share with the DfE, for the purpose of data collections, go to <https://www.gov.uk/education/data-collection-and-censuses-for-schools>.

To find out more about the NPD, go to <https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information>.

For more information about the DfE's data sharing process, please visit:
<https://www.gov.uk/data-protection-how-we-collect-and-share-research-data>

For information about which organisations the department has provided pupil information, (and for which project), please visit the following website: <https://www.gov.uk/government/publications/national-pupil-database-requests-received>

To contact DfE: <https://www.gov.uk/contact-dfe>

Appendix 3: Privacy Notice for Tunbridge Wells Girls' Grammar School (TWGGS) – Workforce

This notice explains what personal data (information) we hold about you, how we collect, how we use and may share information about you. We are required to give you this information under data protection law.

Who are we?

TWGGS collects, uses and is responsible for certain personal information about you. When we do so we are regulated under the General Data Protection Regulation which applies across the European Union (including in the United Kingdom) and we are responsible as 'controller' of that personal information for the purposes of those laws.

The personal information we collect and use

Information collected by us

In the course of employing staff in our school we collect the following personal information when you provide it to us:

- Personal information (such as name, address, contact details, employee or teacher number, national insurance number)
- Characteristics (such as gender, age, ethnic group)
- Contract information (such as start dates, hours worked, post, roles and salary information)
- Work absence information (such as number of absences and reasons)
- Qualifications (and, where relevant, subjects taught)
- Relevant medical information

How we use your personal information

We use your personal information to:

- Enable individuals to be paid
- Support pension payments and calculations
- Enable sickness monitoring
- Enable leave payments (such as sick pay and maternity leave)
- Develop a comprehensive picture of the workforce and how it is deployed
- Inform the development of recruitment and retention policies
- Inform financial audits of the school
- Fulfil our duty of care towards our staff
- Inform national workforce policy monitoring and development

How long your personal data will be kept

We will hold your personal information for 6 years after leaving the school's employment, in line with KCC's personnel retention record keeping guidelines.

Reasons we can collect and use your personal information

We rely on having a legitimate reason as your employer to collect and use your personal information, and to comply with our statutory obligations, and to carry out tasks in the public interest. If we need to collect special category (sensitive) personal information, we rely upon reasons of substantial public interest (equality of opportunity or treatment).

We are required to share information about our workforce members under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

Who we share your personal information with

- Department for Education (DfE)
- Kent County Council Management Information
- Kent County Council Schools Financial Services
- Commissioned providers of personnel and payroll services, Schools Personnel Services and Baxter's
- Harrison Catering Services Ltd and sQuid (on-line payment company used by Harrison Catering for payment of school lunches) – Harrison Catering is contractually engaged to operate catering within school. Any member of staff wishing to use the school canteen needs to pass names to Harrison's for the purpose of setting up/maintaining lunch accounts. Harrison Catering initially provide to sQuid the names of any such members of staff to enable a sQuid account registration number to be generated – this is then provided to staff for them then to register directly with sQuid

- School photographers: an external company (currently Van Cols) takes photographs of individual staff, forms, year groups and the whole school. These photographs are offered to staff and parents for sale, and the individual photographs of staff are held electronically on the school information management system (SIMS) to enable identification. Whole school photographs and year group photographs of Years 11 and U6th are put on display in the school building.

We will share personal information with law enforcement or other authorities if required by applicable law.

The DfE collects and processes personal data relating to those employed by schools and local authorities that work in state funded schools (including all maintained schools, all academies and free schools and all special schools including Pupil Referral Units and Alternative Provision). All state funded schools are required to make a census submission because it is a statutory return under sections 113 and 114 of the Education Act 2005.

The DfE may share information about school employees with third parties who promote the education or well-being of children or the effective deployment of school staff in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance

The DfE has robust processes in place to ensure the confidentiality of our data is maintained and there are stringent controls in place regarding access and use of the data. Decisions on whether DfE releases data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data
- the purpose for which it is required
- the level and sensitivity of data requested: and
- the arrangements in place to store and handle the data

To be granted access to school workforce information, organisations must comply with its strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

Your Rights

Under the GDPR you have rights which you can exercise free of charge which allow you to:

- Know what we are doing with your information and why we are doing it
- Ask to see what information we hold about you (Subject Access Requests)
- Ask us to correct any mistakes in the information we hold about you
- Object to direct marketing
- Make a complaint to the Information Commissioners Office
- Withdraw consent (if applicable)

Depending on our reason for using your information you may also be entitled to:

- Ask us to delete information we hold about you
- Have your information transferred electronically to yourself or to another organisation
- Object to decisions being made that significantly affect you
- Object to how we are using your information
- Stop us using your information in certain ways

We will always seek to comply with your request however we may be required to hold or use your information to comply with legal duties. Please note: your request may delay or prevent us delivering a service to you.

For further information about your rights, including the circumstances in which they apply, see the guidance from the UK Information Commissioners Office (ICO) on individuals' rights under the General Data Protection Regulation.

If you would like to exercise a right, please contact the Data Protection Officer via the school, either in writing, or on dpo@twggs.kent.sch.uk

Keeping your personal information secure

We have appropriate security measures in place to prevent personal information from being accidentally lost, or used or accessed in an unauthorised way. We limit access to your personal information to those who have a genuine business need to know it. Those processing your information will do so only in an authorised manner and are subject to a duty of confidentiality.

We also have procedures in place to deal with any suspected data security breach. We will notify you and any applicable regulator of a suspected data security breach where we are legally required to do so.

Who to Contact and Where to go for Further Information

Please contact the Data Protection Officer via the school, either in writing, or on dpo@twggs.kent.sch.uk to exercise any of your rights, or if you have a complaint about why your information has been collected, how it has been used or how long we have kept it for.

If you would like to get a copy of the information about you that KCC shares with the DfE or post-16 providers or how they use your information, please contact the Information Resilience and Transparency Team at data.protection@kent.gov.uk.

For more information about services for children and young people, please go to: <http://www.kent.gov.uk/education-and-children> or the KCC website at www.kent.gov.uk

The General Data Protection Regulation also gives you right to lodge a complaint with a supervisory authority. The supervisory authority in the UK is the Information Commissioner who may be contacted at <https://ico.org.uk/concerns> or telephone 03031 231113.

For further information visit <https://www.kent.gov.uk/about-the-council/about-the-website/privacy-statement>

For further information about how the Department for Education uses your information:

To find out more about the pupil information we share with the DfE, for the purpose of data collections, go to <https://www.gov.uk/education/data-collection-and-censuses-for-schools>.

To find out more about the NPD, go to <https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information>.

For more information about the DfE's data sharing process, please visit:

<https://www.gov.uk/data-protection-how-we-collect-and-share-research-data>

For information about which organisations the department has provided pupil information, (and for which project), please visit the following website: <https://www.gov.uk/government/publications/national-pupil-database-requests-received>

To contact DfE: <https://www.gov.uk/contact-dfe>