



Gillingham School Dorset

United Learning Data Protection GDPR Policy

Last review:	March 2026
Next review:	March 2027
Signed:	PN/NC/EV Subject to ratification
Approval Committee:	Governing Body

United Learning Data Protection GDPR Policy

Data Protection

Gillingham School holds the legal right and obligation to collect and use personal data relating to students and their families as set out in the General Data Protection Regulations (GDPR). Under GDPR, the lawful basis we rely upon for processing student information are legal obligation, public task and substantial public interest.

Under GDPR there are six data protection principles that we will adhere to:

- 1) We will process data in a fair, lawful and transparent manner.
- 2) We will collect data for specified, explicit and legitimate purposes and it will not be further processed in a manner that is incompatible with those purposes.
- 3) We will collect an amount of data which is adequate, relevant and limited to what is necessary.
- 4) We will collect data accurately and where necessary keep it up to date.
- 5) We will keep data in a form permitting identification for no longer than is necessary.
- 6) We will process data in a manner ensuring appropriate security of personal data.

Underpinning these principles, individuals have five main rights within GDPR, centered around:

1. To access their data
2. To rectify their data (correcting data)
3. To erase their data
4. To restrict the processing of their data
5. To withdraw their consent for data use

The Governing Body of the school has overall responsibility for ensuring that records are maintained, including security and access arrangements, in accordance with Education Regulations and all other statutory provisions. The Head Teacher and Governors of the School intend to comply fully with the requirements and principles of GDPR and both the Data Protection Act 1998 and the Data (Use and Access) Act 2025 which adds targeted amendments, modernizing them in line with technological advancements. All school staff are aware of their duties and responsibilities within these guidelines. This policy and general procedures are reviewed regularly and at least annually.

Part B of this document comprises the Gillingham School Privacy Notice, which is also published separately on the school website. This outlines 'Why and How' we process data and our legal basis for doing so.

Please also see the **Biometric Information Policy**.

Data accuracy

Data held will be as accurate and up to date as is reasonably possible. If a data subject informs the school of a change of circumstances, their computer (Arbor) record will be updated as soon as it is practicable. Updated student data can also be communicated to the school using the EduLink App or website.

Data Retention

Data held about individuals will not be kept for longer than necessary for the purposes registered. It is the duty of administrative staff, Year Heads, Heads of Department and Senior Staff to ensure that obsolete data is properly erased and/or destroyed as appropriate, using the 'Retention Guidelines for Schools' documentation.

Data and Computer Security

Gillingham School undertakes to ensure security of personal data in the following ways:

1. Physical Security

- Appropriate building security measures are in place, such as alarms, window bars, deadlocks and computer hardware cable locks.
- Only authorised people are allowed in the computer server rooms.
- Files and other personal data are stored securely when not in use.
- Visitors to the school are required to sign in and out, to wear identification badges whilst in the school and are, where appropriate, accompanied.

2. Electronic Security

- Clear data protection is closely linked to cyber security, and we will be mindful of the advice in the '10 Steps to Cyber Security' leaflet produced by the National Cyber Security Centre.
- Gillingham School uses various in-perimeter and out-of-perimeter security systems to mitigate against ransomware, malware and viruses.
- Staff training, advice and guidance on e-security are available from the IT Services Department in school.
- Security software is installed on all computers containing personal data.
- Only authorised users are allowed access to the computer files.
- Computer files are 'backed up' regularly.
- Clearly, many documents in school contain sensitive and personal data. (For example, EHCPs, SEN statements and annual reviews, exclusion letters). Great care must be taken when, on very rare occasions, copies of these documents are taken off-site.
- Use of memory sticks is strongly discouraged, and any containing of personal and sensitive data should be encrypted and documents protected. Technical assistance with this is available from the IT Services Department in school. Staff are advised to use remote access to view data away from the school, rather than transporting data via a memory stick.
- Staff must ensure that when staff or pupils' information (electronically or otherwise) is taken off site it is always kept secure.

3. Procedural Security

- All staff are informed of their Data Protection obligations and their knowledge updated as necessary. Staff are regularly reminded about their responsibilities regarding GDPR.
- Staff are aware that individuals can be personally liable in law under the terms of the Data Protection Acts and that a deliberate breach of this Data Protection Policy will be treated as disciplinary matter, and serious breaches could lead to dismissal.
- To be given authorised access to the computer, staff will have to undergo checks and will agree to a confidentiality agreement (this is done when staff log on to the computer).
- Staff should not leave their computers logged on to personal data (for example, SIMS) when they are not present in the room. Use of 'Windows' 'L' to lock a workstation is encouraged.
- Printouts as well as source documents containing personal data are stored securely and shredded before disposal according to our retention schedule. (For example, personal data recorded for school trips). Where possible, staff should avoid printing documents containing personal data.
- Students' school record files should not be taken off-site except under exceptional circumstances.
- Staff should avoid leaving documents containing personal and sensitive data in places easily seen by others; for example, they are left on desks at the end of the day.
- Staff should take extra care to ensure that emails are sent to the intended recipient only.

- As outlined in the school's Privacy Policy, we will ensure that any 'third party' contractors handling data are GDPR compliant. When data is required to be shared, the same data protection standards that Gillingham School upholds are imposed on the processor. The minimum amount of data is transferred, such as student name and date of birth, as necessary.
- When mandatory the school will ensure to have a Data Protection Impact Assessment in place. Instances where this applies are the use of CCTV, the use of CCTV in washrooms and the use of biometrics. A summary of these documents is available on request.
- Gillingham School have considered the need for using CCTV and have decided it is necessary to help deter crime, protect the safety of individuals, or the security of premises. We will not use the system for any incompatible purposes, and we conduct regular reviews of our use of CCTV to ensure that it is still necessary and proportionate. Gillingham School notifies all pupils, staff, and visitors of the purpose for collecting CCTV images via signage and letters. Cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose. All CCTV footage may be kept for 30 days for security purposes; a nominated controller is responsible for keeping records secure and allowing access to images. These will be viewed on a case-by-case basis and only when appropriate. 22 Under Article 15 of the UK GDPR law, the right of access gives individuals the right to obtain a copy of their personal data from CCTV unless an exemption applies. This can be provided either in permanent form, or through arrangement to view the information. An exemption would include if the footage included other people. This will then need to redact so they cannot be identified. Where this is not possible or appropriate, we will consider asking for their consent before releasing this. Where this is not possible or appropriate, we will balance the requester's rights against any third-party rights to privacy and decide if it's reasonable to share the footage without their consent. The reasons for any decision will be documented.
- At present the school does not use any Automated Decision-Making systems without human intervention but will keep this under review and incorporate guidance when it becomes necessary.
- Marketing and Cookies. We comply with PECR rules for electronic marketing and cookies. When DUAA cookie changes commence, certain low risk cookies (e.g., statistical or functionality) may be set without prior consent, provided we meet transparency and opt-out requirements; keep banners/notices under review. PECR fines now align with UK GDPR.
- Use of Artificial Intelligence (AI). Our school may make use of artificial intelligence (AI) tools to support teaching, learning, and administrative functions. Any use of AI will comply with the UK GDPR and Data Protection Act 2018.
- Personal or sensitive data must not be entered into AI systems unless a Data Protection Impact Assessment (DPIA) has been completed and appropriate safeguards are in place.
- AI tools will only be used following assessment of risks relating to accuracy, fairness, transparency and data security.
- All AI-generated content will be reviewed by staff before use.
- No automated decision-making that produces legal or significant effects on individuals will be carried out using AI.

This aligns with DfE and ICO expectations and current sector practice.

Subject Access Requests

Data subjects have a right to access their own personal data. To ensure that people receive only information about themselves it is essential that a formal system of requests is in place. Requests from pupils will be processed as any subject access request as outlined below and the copy will be given directly to the pupil, unless the pupil does not understand the nature of the request. Requests from pupils who do not appear to understand the nature of the request will be referred to by their parents or carers.

Requests from parents in respect of their own child will be processed as requests made on behalf of the data subject (the child) and the copy will be sent in a sealed envelope to the requesting parent when appropriate.

Processing Subject Access Requests

Requests for access must be made in writing.

Pupils, parents or staff should ask for a Data Subject Access form, available from Mrs. A Stickland. Completed forms should be returned to her. Provided that there is sufficient information to process the request, an entry will be made in the Subject Access Logbook, showing the date of receipt, the data subject's name, the name and address of requester (if different), the type of data required (e.g. Student Record, Personnel Record), and the planned date of supplying the information (normally not more than 20 working days, therefore not including school holidays, from the request date). Should more information be required to establish either the identity of the data subject (or agent) or the type of data requested, the date of entry in the log will be the date on which sufficient information has been provided. A reasonable charge will be incurred to cover the costs of photocopying.

In the case of any written request from a parent regarding their own child's record, access to the record will be provided in accordance with the current Education (Pupil Information) Regulations.

Disclosure of Data

A "legal disclosure" is the release of personal information to someone who requires the information to do his or her job within or for the school.

An "illegal disclosure" is the release of information to someone who does not need it, or has no right to it, or one which falls outside the school's registered purposes. It is worth noting that comments on Facebook / Twitter etc. which disclose privileged personal data would fall into the category of 'illegal disclosure'. As required under GDPR, we will report a data breach / illegal disclosure to the ICO within 72 hours where the loss of data is more than likely 'to result in a risk to the rights and freedoms of natural persons', for example damage to reputation, financial loss or discrimination. We will also inform the individuals involved.

Contacts in school are:

Ms. E Vallender **Data Protection Officer**

Mrs. N Cross **Assistant Headteacher**

Catherine Doble **Personal Assistant to the Headteacher**

General information about General Data Protection Regulation (GDPR) and The Data Protection Act can be obtained from the Information Commissioner's Office (ICO) www.ico.org.uk

PART B

Gillingham School Privacy Notice

Why and how we use student information.

This notice is intended to provide information about how the Academy will use or "process" personal data about individuals including current, past and prospective pupils (referred to in this notice as "pupils") and their parents, carers or guardians (referred to in this notice as "parents").

Responsibility for Data Protection

The Data Controller for personal information held by Gillingham School is United Learning Trust (ULT). ULT is registered with the Information Commissioner's Office (ICO). The registration number is Z7415170.

The Company Secretary is the Data Protection Officer (DPO) and is responsible for ensuring that ULT complies with the Data Protection Law. They can be contacted on company.secretary@unitedlearning.org.uk or 01832 864538.

Emma Vallender evallender@gillingham-dorset.co.uk is responsible for ensuring that the Academy complies with ULT's policies and procedures in relation to Data Protection.

Why we collect and use Personal Data about pupils and parents

Gillingham School and United Learning Trust collect, create and hold personal information relating to our pupils and may also receive information about them from their previous school/Academy, local authority and/or the Department for Education (DfE). We also collect and hold personal information about our pupil's parents and carers. We use this personal data to:

- Provide education services (including SEN), career services and extra-curricular activities to pupils; monitor pupils' progress and educational needs;
- To safeguard pupils' welfare and provide appropriate pastoral (and where necessary, medical) care.
- To enable pupils to take part in national or other assessments, and to publish the results of public examinations or other achievements of pupils at the Academy.
- To maintain relationships with alumni and the school community.
- For the purposes of management planning and forecasting, research and statistical analysis and to enable ULT to monitor the Academy's performance.
- To monitor use of the Academy's IT systems in accordance with the Academy's Acceptable Use Policy.
- To receive information about current and prospective pupils from any educational institution that they attended.
- To confirm the identity of prospective pupils and their parents.
- To make use of images of pupils in print and digital communications, and for promotion and marketing, in accordance with the Academy's/School's policy on taking, storing and using images of children.
- To create invoices and process payments for services such as school meals, school trips etc.
- For security purposes, and for regulatory and legal purposes (for example child protection and health and safety) and to comply with its legal obligations.
- To receive reports from any organisation that may be working with your child.
- Where otherwise reasonably necessary for the Academy's purposes, including to obtain appropriate professional advice and insurance for the Academy.
- To keep you updated about the activities of the Academy including by sending updates and newsletters by email and post.
- To organise trips and visits both in the UK and abroad.

The categories of personal data that we process

The types of personal data processed by the Academy include:

1. Names, addresses, telephone numbers, email addresses and other contact details.
2. Academic records and national curriculum assessment results, including examination scripts and marks.
3. Personal characteristics such as your ethnic group, religious beliefs, any special educational needs you may have and any relevant medical information.
4. Attendance information, behavioural records, any exclusion information.
5. Information provided by previous educational establishments and or other professionals or organisations working with pupils.
6. Where pupils go after they leave the Academy.
7. 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.
8. Images captured by the Academy's CCTV system in accordance with the CCTV policy.
9. Still and moving images in accordance with the Academy's image use policy.

The legal basis for the processing of pupil and parent data

The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller and where necessary to comply with our legal obligations.

Information relating to racial or ethnic origin, religious beliefs or health (point 3) will only be processed with the explicit consent of the pupil or the pupil's parents or when it is necessary for carrying out our legislative obligations. Further information regarding the purposes for which these data would be processed will be provided with the data collection form.

Data Retention Periods

The pupil's educational record will move with the pupil to their next school/Academy. Where the school/Academy is the last school that the pupil attends the records will be kept until the pupil is 25 years old. However, we are required to retain some Special Educational Needs and Disability information for longer than this. Student files are stored securely and paper files destroyed.

Admissions information will be retained for one year post successful admission or closure of appeal.

Information relating to financial transactions will be kept for 7 years.

For further information on how long we keep personal data for please refer to our records retention schedule which can be found [Records Management Retention Schedule.pdf](#)

Data Security

ULT has in place technical and organisational measures that ensure a level of security appropriate to the sensitive nature of the personal data that we process. For further information regarding how we keep personal data secure please refer to our security of personal data policy.

Data Processors

We use third party data processors to provide us with a variety of services¹. This use of data processors will only take place if it is in compliance with the UK GDPR and the Data Protection Act 2018 (and any subsequent legislation related to data protection in applicable jurisdictions).

Decisions on whether we contract with these third-party processors are subject to a robust approval process and are based on a detailed assessment of the purpose for which the data processing is required, the level and sensitivity of data involved and the arrangements in place to store and handle the data. To be granted access to pupil level data, data processors must comply with strict terms and conditions covering the confidentiality and handling of data, security arrangements and retention and use of the data.

We currently use the following data processors:

Arbor, Microsoft 365, Sparx, Wonde, EduLink (including IpayImpact), CPOMs

Who we share pupil information with We do not share information about our students with anyone without consent unless the law and our policies allow us to do so.

We routinely share pupil information with:

- Schools that the students attend after leaving us
- Our Local Authority (Dorset County Council)
- Other Local Authorities in which our students live (Wiltshire, Somerset)
- Youth support services (students aged 13+)
- The Department for Education (DfE)
- Exam Boards
- The Education and Skills Funding Agency
- Aspens (School Catering providers)
- School transport companies
- Curriculum resource providers, such as GCSEPod and Sparx.
- NHS, the school nurse and other health professionals as necessary

Data (such as student names) may be shared with educational websites to enable students to log in to these in lessons or for home learning.

When data is required to be shared, the same data protection standards that Gillingham School upholds are imposed on the processor. The minimum amount of data is transferred, such as student name and date of birth, as necessary.

DfE may also share pupil level personal data that we supply to them, with third parties. This will only take place where legislation allows it to do so, and it is in compliance with the UK GDPR and the Data Protection Act 2018 (and any subsequent legislation related to data protection in applicable jurisdictions)..

Decisions on whether DfE releases this personal data to third parties are subject to a robust approval process and are 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 level data, requestors must comply with strict terms and conditions covering the confidentiality and handling of data, security arrangements and retention and use of the data.

For more information on how this sharing process works, please visit: <https://www.gov.uk/guidance/national-pupil-database-apply-for-a-data-extract>

For information on which third party organisations (and for which project) pupil level data has been provided to, please visit: <https://www.gov.uk/government/publications/national-pupil-database-requests-received>

If you need more information about how our local authority and/or DfE collect and use your information, please visit:

- our local authority [School organisation team privacy notice - Dorset Council](#) or the DfE website at <https://www.gov.uk/data-protection-how-we-collect-and-share-research-data>

We will not give information about our pupils to any other third parties without your consent unless the law and our policies allow us to do so.

Rights of the Data Subject

Data protection legislation gives individuals certain rights which are detailed below. If you wish to exercise these rights, please contact Catherine Doble (cdoble@gillingham-dorset.co.uk)

Right of access to personal data “subject access request”

You have the right to access the personal data that the Academy holds about you. Requests may be made in writing or orally (if requested orally we will make a record of that request to ensure it is met within the required timescale). Parents also have the right to request the personal data held about their children (If your child is over the age of 12 they will need to decide whether to consent to the request). We take the security of personal data seriously so we may ask you for proof of identity to verify that you are entitled to the information requested.

Right to withdraw consent

Where we have obtained your consent to specific processing activities you may withdraw this consent at any time.

Right to rectification

You have the right to have the personal data that we hold about you rectified if it is inaccurate or incomplete. We will respond to such requests within one month.

Right to erasure

You have the right to have personal data erased in certain specific circumstances. If you make such a request, we will consider whether the right to erasure applies and give you a full and reasoned response.

Right to restrict processing

In certain circumstances you have the right to request that we restrict the processing of your personal data. If you make such a request, we will consider whether the right to restrict processing applies and give you a full and reasoned response.

Further Information

For further information regarding your rights please refer to our rights of the data subject policy.

If you disagree with a decision that we have taken regarding the processing of your personal data please contact ULT’s Company Secretary, Alison Hussain, on 01832 864538 or company.secretary@unitedlearning.org.uk.

You also have the right to lodge a complaint with the information Commissioners Office on 0303 123 1113 or <https://ico.org.uk/for-the-public/>.

Contact

If you would like to discuss anything in this Privacy Notice, please contact Ms Emma Vallender (Data Protection Officer) at the school.

Appendix 1: Taking, storing and using images of children

This appendix applies to all staff who may capture or process images of pupils to ensure the acceptable, safe use and storage of all images within the school. This includes the management, implementation, monitoring and review of all protocols.

We take and store images for several purposes:

- For identification purposes
- To take images of pupils, individually or in groups, as part of the school’s record and as a service for parents
- For security via CCTV recordings
- For teaching and learning purposes
- For use in celebration and promotion of activities in school

For the purposes of identification, record, security and teaching and learning, our legal basis for processing is public task, because we need to process these images as part of running Gillingham School.

Photographs taken in school as a service for parents (such as class photos) are processed on the basis of legitimate interest, because this is an activity that people might reasonably expect us to perform.

We will ask for consent to use images in promotional material.

How we use Your Data

The data controller for personal information held by Gillingham School is United Learning Trust (ULT). ULT is registered with the Information Commissioner's Office (ICO). The registration number is Z7415170. The Company Secretary, Alison Hussain, is responsible for ensuring that ULT complies with the Data Protection Law. She can be contacted on company.secretary@unitedlearning.org.uk or 01832 864538.

All images will be used in a manner respectful of the eight Data Protection Principles. This means that images will be:

- fairly and lawfully processed
- processed for limited, specifically stated purposes only
- used in a way that is adequate, relevant and not excessive
- accurate and up to date
- kept on file for no longer than is necessary
- processed in line with an individual's legal rights
- kept securely
- adequately protected if transferred to other countries.

Roles and Responsibilities

Paul Nicholson **Headteacher** has overall responsibility for ensuring the acceptable, safe and lawful use, storage and disposal of all images taken within the school.

Colin Gordon **DSL** is responsible for ensuring that the use of images complies with safeguarding requirements and does not place children at risk.

Emma Vallender **DPO** is responsible for advising on compliance with UK GDPR and the Data Protection Act 2018, including the lawful processing, storage, retention and disposal of images.

Mel Marshall **Deputy Head** is responsible for the school's website, social media and communications is responsible for ensuring that images published on the school's website, social media channels and other public-facing platforms comply with consent requirements, safeguarding considerations and this policy.

Josh Bache **IT Manager** is responsible for maintaining secure systems for the storage and transfer of images.

How we seek your consent for images used for promotion

- Written parental permission will be sought on entry to the school. A record of all consent details will be kept securely on EduLink.
- Should permission later be withdrawn by parents/carers, records will be updated and the relevant staff informed, and no further images of the pupil concerned will be captured for use in publicity. *(Please note that withdrawal of images already in circulation may not be possible.)*
- We will always make individuals aware if photography is taking place and will talk about how and why we are taking the images in an age-appropriate way.
- We will always respect the individual and will never take images of anyone against their wishes.
- When taking images, careful consideration will be given before involving very young or vulnerable children who may be unable to question why or how activities are taking place.
- Photography is not permitted in sensitive areas such as changing rooms, toilets, etc.

There are always some risks associated with the distribution of images. These measures help to mitigate those risks, but you should make sure you are comfortable with your child being featured in images before you give consent.

How we use images for promotion

Images are a way for us to celebrate achievement, keep parents and communities informed about our activities, and raise our profile. Parents and families and the children themselves often derive great pleasure from seeing their loved ones in print or on a website.

- Images may be included in print or digital media. Examples might include printed publications; websites; adverts; in communications channels such as newsletters or social media; as part of wall displays; or to accompany stories in the media.
- Children's full names will not be associated with photographs except where directly relevant.

Capture of images by Parents/Carers

- Parents/Carers are permitted to take photographs or video footage of events for private use only.
- Parents/Carers must not share images of any other pupil on social media.
- Parents/Carers are not permitted to take photographs in sensitive areas such as changing rooms, toilets, swimming areas etc.
- Parents/Carers who are using photographic equipment must be mindful of others when capturing images.
- Parents/Carers may contact the school's DSL to discuss any concerns regarding the use of images.

Capture of images by children

- We will discuss and agree age-appropriate acceptable use rules with children regarding the use of cameras, such as places children must not capture images (eg unsupervised areas, toilets etc).
- All staff will be made aware of the acceptable use rules regarding children's use of cameras and will ensure that children are appropriately supervised when taking images for official or curriculum use.
- Members of staff will role model positive behaviour to the children by encouraging them to ask permission before they take any photos.
- Images taken by children which are used for school purposes will be processed and stored in accordance with this policy.

Use of Closed-Circuit Television (CCTV)

For information on how we capture and process images through CCTV, please refer to section 3 of the GDPR policy.

Further information

You can read more about how we capture, use, process and store images in the following policies:

- Safeguarding and Child Protection Policy
- Staff code of conduct
- The Gillingham School Privacy Notice is contained within this Data Protection GDPR Policy. It explains how personal information, including photographs and video images, is collected, used, stored and shared. The Privacy Notice is also on the website.

Appendix 2: Parental consent to use pupil photos and videos (images) for promotion

Parental consent for the use of pupil images is sought for all students on roll. Parents give consent when completing the school admissions form as follows:

Use of information and image (including photographs and video recordings)

Please indicate below whether you have given your consent in each case by ticking the box on the right-hand side and sign and date the form on the last page.

I give consent for my child's image and/or work to be used as part of school wall displays/class activities/formal class/whole school photographs/in school media productions.	
I give consent for my child's image (not named) to be used on the school website/newsletter/social media (e.g. Facebook/Instagram/Twitter).	
I give consent for my child's image (not named) to be used in external media, e.g. local newspaper press release.	

If parents wish to withdraw consent, they need to contact Roxy Clifton on roxy.clifton@gillingham-dorset.co.uk

Should parents withdraw consent, no further images of the pupil concerned will be captured for use in publicity.

Gillingham School and United Learning will stop using the image in future publications where reasonably practicable, but previously published copies may remain accessible.

The data controller for personal information held by Gillingham School is United Learning Trust (ULT). ULT is registered with the Information Commissioner's Office (ICO). The registration number is Z7415170. The Company Secretary, Alison Hussain, is responsible for ensuring that ULT complies with the Data Protection Law. She can be contacted on company.secretary@unitedlearning.org.uk or 01832 864538.