SUMMERHILL SCHOOL

Founded 1921

School Office
Summerhill School
Westward Ho
LEISTON
Suffolk IP16 4HY
Tel/Fax: 00 (44) 1728 830540
E-mail: office@summerhillschool.co.uk

Principal
Zoë Readhead
Tel: 00 (44) 1728 830030
E-mail: zoe@summerhillschool.co.uk
www.summerhillschool.co.uk

DATA PROTECTION POLICY

IT

January 2026

The need for the policy

All Summerhill School information communication technology (IT) facilities and information resources remain the property of Summerhill School and not of particular individuals, teams or departments. By following this policy, we will help ensure that IT facilities are used:

Legally; securely; without undermining Summerhill School; effectively; in a spirit of co-operation, trust and consideration for others; so that they remain available.

The policy relates to all IT facilities and services provided by Summerhill School, although special emphasis is placed on email and the internet. All employees, volunteers, and any other users of our IT are expected to adhere to the policy.

1. Security

1.1. As a user of Summerhill's equipment and services, you are responsible for your activity.

1.2. Do not disclose personal passwords or other security details to other employees, or external agents, and do not use anyone else's log-in; this compromises the security of Summerhill School. If someone else gets to know your password, ensure that you change it.

1.3. If you intend to leave your PC or workstation unattended for any reason, you should lock the screen to prevent unauthorized access. If you fail to do this, you will be responsible for any misuse of it while you are away. Logging off is especially important where visitors to the school have access to the screen in your absence.

2. Use of Email

2.1. When to use email

2.1.1. Summerhill School has a policy for the use of email whereby employees must ensure that they:

2.1.1.1. comply with current legislation.

2.1.1.2. use email in an acceptable way.

2.1.1.3. do not create unnecessary business risk to Summerhill School by their misuse of the internet.

2.1.1.4. professional communication via email, between external parties and school community members, should be made using @summerhillschool.co.uk official email accounts

2.2. Unacceptable behaviour See *Code of Conduct* (Ba.2)

2.3. Confidentiality

2.3.1. Always exercise caution when committing confidential information to email since the confidentiality of such material cannot be guaranteed.

2.4. General points on email use

2.4.1. When publishing or transmitting information externally be aware that you are representing Summerhill School and could be seen as speaking on Summerhill School's behalf. Make it clear when opinions are personal. If in doubt, consult Zoe, Will or Henry.

2.4.2. Check your inbox at regular intervals during the working day. Your inbox should be checked regularly so that there is no backlog and daily workflow is good. Please be aware it is not expected you answer emails outside of work hours.

2.4.3. Keep electronic files of electronic correspondence, only retaining what you need to. Do not print it off and keep paper files unless absolutely necessary.

2.4.4. Treat others with respect and in a way in which you would expect to be treated yourself (e.g. do not send unconstructive feedback, argue, or invite colleagues to make public their displeasure at the actions / decisions of a colleague).

3. Google Workspace

3.1. Keep master copies of important data on Summerhill School's Google environment and not solely on your PC's local hard drive or portable disks. Not storing data on Summerhill's Google environment means it will not be backed up and is therefore at risk.

3.2. To prevent unauthorised access to Summerhill's Google environment, keep all information such as login names and passwords confidential and do not disclose them to anyone.

3.3. Select passwords that are not easily guessed, e.g. do not use your house or telephone number and do not choose consecutive or repeated numbers. Other technical security requirements may be requested of staff, and these should be complied with.

3.4. Avoid writing down or otherwise recording any network access information where possible. Any information that is written down must be kept in a secure place and disguised so that no other person is able to identify what it is.

3.5. Protect Summerhill School's information and data at all times, including any printed material produced while using the Summerhill's Google environment. [Take particular care when access is from a non-office environment].

3.6. Care should be taken when working on laptops in public places (e.g. trains) that any sensitive details are not visible to other people.

3.7. Summerhill School retains and has the ability to review at the principal's discretion data stored in Google Workspace, potentially including after a user has deleted it.

4. CCTV

4.1. Signage must be placed clearly around the school entrances. Further, information as to who to contact and for how long information is kept must also be displayed.

4.2. Summerhill School will not disclose CCTV images of identifiable people to the media - or to put them on the internet - for entertainment. Images released to the media to help identify a person are usually disclosed by the police.

4.3. Summerhill School may need to disclose CCTV images for legal reasons – for example, crime detection. Once they have given the images to another organisation, then that organisation must adhere to the Data Protection Act in their handling of the images.

5. Online purchasing

5.1. Any users who place and pay for orders online using personal details do so at their own risk and Summerhill School accepts no liability if details are fraudulently obtained whilst the user is using Summerhill School's equipment.

6. Agreement

6.1. All employees, volunteers, visitors, contractors or temporary employees who have been granted the right to use the Summerhill School's IT systems are required to sign this agreement confirming their understanding and acceptance of this policy.

Data Protection

1. Introduction

1.1. Summerhill School ("the School") collects and uses certain types of personal information about staff, pupils, parents and other individuals who come into contact with the School in order to provide education and associated functions. The School may be required by law to collect and use certain types of information to comply with statutory obligations related to employment, education and safeguarding, and this policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the General Data Protection Regulation ("GDPR") and other related legislation including the Data (Use and Access) Act 2025 ('DUAA') which amends the existing data protection framework. The Data (Use and Access) Act 2025 came into law on June 19, 2025, and its provisions are being phased in over time.

1.2. This policy will be updated as necessary to reflect best practice, or amendments made to data protection legislation, and will be reviewed every year.

1.3. The school's data protection officer is Henry Readhead, and his contact details are:

Telephone: 01728 830540.

Email: henry.r@summerhillschool.co.uk

2. Personal Data

2.1. 'Personal data' is information that identifies an individual and includes information that would identify an individual to the person to whom it is disclosed because of any special knowledge that they have or can obtain.

A sub-set of personal data is known as **'special category personal data'**. This special category data is information that relates to:

2.1.1. Nationality.

2.1.2. Physical or Mental health.

2.2. Special Category information is given special protection, and additional safeguards apply if this information is to be collected and used.

2.3. Information relating to criminal convictions shall only be held and processed where there is legal authority to do so.

2.4. The School does not intend to seek or hold sensitive personal data about staff or students except where the School has been notified of the information, or it comes to the School's attention via legitimate means (e.g. a grievance) or needs to be sought and held in compliance with a legal obligation or as a matter of good practice. Staff or students are under no obligation to disclose to the School their race or ethnic origin, political or religious beliefs, whether or not they are a trade union member or details of their sexual life (save to the

extent that details of marital status and/or parenthood are needed for other purposes, e.g. pension entitlements).

3. The Data Protection Principles

3.1. The six data protection principles as laid down in the GDPR are followed at all times:

3.1.1. Personal data shall be processed fairly, lawfully and in a transparent manner, and processing shall not be lawful unless one of the processing conditions can be met:

3.1.2. Personal data shall be collected for specific, explicit, and legitimate purposes, and shall not be further processed in a manner incompatible with those purposes.

Under DUAA certain further processing may be permissible for recognised purposes such as scientific, historical, statistical research or archiving in the public interest provided appropriate safeguards are applied (e.g. pseudonymisation, minimisation, access controls).

Compatibility assessments must be documented and any use of personal data beyond the original purpose must be justified and recorded in accordance with DUAA's strengthened accountability requirements.

3.1.3. Personal data shall be adequate, relevant, and limited to what is necessary for the purpose(s) for which it is being processed.

3.1.4. Personal data shall be accurate and, where necessary, kept up to date.

3.1.5. Personal data processed for any purpose(s) shall not be kept for longer than is necessary for that purpose/those purposes.

3.1.6. Personal data shall be processed in such a way that ensures appropriate security of the data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

3.2. In addition to this, the School is committed to ensuring that at all times, anyone dealing with personal data shall be mindful of the individual's rights under the law.

3.3. The School is committed to complying with the principles in 3.1 at all times.

This means that the School will:

3.3.1. inform individuals as to the purpose of collecting any information from them, as and when we ask for it.

3.3.2. be responsible for checking the quality and accuracy of the information.

3.3.3. regularly review the records held to ensure that information is not held longer than is necessary, and that it has been held in accordance with the data retention policy. (see *Information Retention and Destruction Policy*).

3.3.4. ensure that when information is authorised for disposal it is done appropriately.

3.3.5. ensure appropriate security measures to safeguard personal information whether it is held in paper files or on our computer system and follow the relevant security policy requirements at all times.

3.3.6. share personal information with others only when it is necessary and legally appropriate to do so.

3.3.7. set out clear procedures for responding to requests for access to personal information known as subject access requests.

3.3.8. report any breaches of the GDPR in accordance with the procedure in paragraph 11 below.

4. Conditions for Processing of the First Data Protection Principle

4.1. The individual has given consent that is specific to the particular type of processing activity, and that consent is informed, unambiguous and freely given. *or*

4.2. The processing is necessary for the performance of a contract, to which the individual is a party, or is necessary for the purpose of taking steps with regards to entering into a contract with the individual, at their request. *or*

4.3. The processing is necessary for the performance of a legal obligation to which we are subject. *or*

4.4. The processing is necessary to protect the vital interests of the individual or another.

4.5. 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 us. *or*

4.6. The processing is necessary for a legitimate interest of the School or that of a third party, except where this interest is overridden by the rights and freedoms of the individual concerned. 'Legitimate interests', includes **"recognised legitimate interest"** introduced by DUAA (for processing serving a broadly accepted purpose in the public or organisational interest), provided these are not overridden by the rights of the data subject.

5. Use of Personal Data by the School

5.1. The School holds personal data on pupils, staff and other individuals such as visitors. In each case, the personal data must be treated in accordance with the data protection principles as outlined in paragraph 3.1 above.

Pupils

5.2. The personal data held regarding pupils includes contact details, assessment / examination results, attendance information, characteristics such as nationality, special educational needs, any relevant medical information, and photographs.

5.3. The data is used in order to support the education of the pupils, to monitor and report on their progress, to provide appropriate pastoral care, and to assess the performance of the School as a whole, together with any other uses normally associated with this provision in a school environment.

5.4. Make personal data, including sensitive personal data, available to staff for planning curricular or extra-curricular activities.

5.5. In particular, the School may use photographs of pupils in accordance with the photograph policy.

5.6. Any wish to limit or object to any use of personal data should be notified to Henry Readhead in writing, which notice will be acknowledged by the School in writing. If, in the view of Henry, the objection cannot be maintained, the individual will be given written reasons why the School cannot comply with their request.

Staff

5.7. The personal data held about staff will include contact details, employment history, information relating to career progression, information relating to DBS checks, photographs.

5.8. The data is used to comply with legal obligations placed on the School in relation to employment, and the education of children in a school environment. The School may pass information to other regulatory authorities where appropriate and may use names and photographs of staff in publicity and promotional material. Personal data will also be used when giving references.

5.9. Staff should note that information about disciplinary action may be kept for longer than the duration of the sanction. Although treated as "spent" once the period of the sanction has expired, the details of the incident may need to be kept for a longer period.

5.10. Any wish to limit or object to the uses to which personal data is to be put should be notified to the school office who will ensure that this is recorded and adhered to if appropriate. If the management is of the view that it is not appropriate to limit the use of personal data in the way specified, the individual will be given written reasons why the School cannot comply with their request.

Other Individuals

5.11. The School may hold personal information in relation to other individuals who have contact with the school, such as volunteers and guests. Such information shall be held only in accordance with the data protection principles and shall not be kept longer than necessary.

5.12. The School may hold CCTV information in regards to vehicles owned by members of the public or businesses visiting the school or going about school business. This information is kept for no longer than a month, unless there is legal reason to do so.

6. Security of Personal Data

6.1. The School will take reasonable steps to ensure that members of staff will only have access to personal data where it is necessary for them to carry out their duties. All staff will be made aware of this policy and their duties under the GDPR. The School will take all reasonable steps to ensure that all personal information is held securely and is not accessible to unauthorised persons.

DUAA explicitly recognises that children's personal data require enhanced protection. Thus, additional safeguards are applied for educational apps, online learning platforms, edtech tools, and any processing of pupils' data.

Further, privacy notices are child-friendly and clearly explain rights and parental / guardian consent is applied where required by law and DUAA guidance.

6.2. For further details as regards security of IT systems, please refer to the IT Policy.

7. Confidentiality of Pupil Concerns

7.1.Where a pupil seeks to raise concerns confidentially with a member of staff and expressly withholds their agreement to their personal data being disclosed to their parents or guardian, the School will maintain confidentiality unless it has reasonable grounds to believe that the pupil does not fully understand the consequences of withholding their consent, or where the School believes disclosure will be in the best interests of the pupil or other pupils.

8. Subject Access Requests (SARs)

The Data (Usage and Access) Act codifies existing guidance from the ICO about SARs. This means that when someone (e.g. a parent, former pupil, staff member etc.) requests all personal data a school holds about them, the school must only conduct 'reasonable and proportionate' searches.

8.1. Anybody who makes a request to see any personal information held about them by the School is making a subject access request. All information relating to the individual, including that held in electronic or manual files should be considered for disclosure.

8.2. All requests should be sent to Henry within 3 working days of receipt by the office and must be dealt with in full without delay and at the latest within one month of receipt.

8.3. Where a child or young person does not have sufficient understanding to make his or her own request (usually those Cottage age and under, or House and over but with a special educational need which makes understanding their information rights more difficult), a person with parental responsibility can make a request on their behalf. Henry must, however, be satisfied that:

8.3.1. the child or young person lacks sufficient understanding, and the request made on behalf of the child or young person is in their interests.

8.4. Any individual, including a child or young person with ownership of their own information rights, may appoint another person to request access to their records. In such circumstances the School must have written evidence that the individual has authorised the person to make the application and Henry must be confident of the identity of the individual making the request and of the authorisation of the individual to whom the request relates.

8.5. Access to records will be refused in instances where an exemption applies, for example, information sharing may place the individual at risk of significant harm or jeopardise police investigations into any alleged offence(s).

8.6. An individual only has the automatic right to access information about themselves, and care needs to be taken not to disclose the personal data of third parties where consent has not been given, or where seeking consent would not be reasonable, and it would not be appropriate to release the information. Particular care must be taken in the case of any complaint or dispute to ensure confidentiality is protected.

8.7.All files must be reviewed by Henry before any disclosure takes place. Access will not be granted before this review has taken place.

8.8. Where all the data in a document cannot be disclosed, a permanent copy should be made and the data obscured or retyped if this is more sensible. A copy of the full document and the altered document should be retained, with the reason why the document was altered.

9. Exemptions to Access by Data Subjects

9.1. Where a claim to legal professional privilege could be maintained in legal proceedings, the information is likely to be exempt from disclosure unless the privilege is waived.

9.2. There are other exemptions from the right of subject access. If we intend to apply any of them to a request, then we will usually explain which exemption is being applied and why.

9.3. Where a release would come into conflict with the school's Community Life policy and Summerhill General policy

10. Other Rights of Individuals

10.1. The School has an obligation to comply with the rights of individuals under the law, and takes these rights seriously. The following section sets out how the School will comply with the rights to:

10.1.1. object to processing.

10.1.2. rectification.

10.1.3. erasure and

10.1.4.data portability.

Right to object to processing

10.2. An individual has the right to object to the processing of their personal data on the grounds of pursuit of a public interest or legitimate interest (grounds 4.5 and 4.6 above) where they do not believe that those grounds apply.

10.3. Where such an objection is made, it must be sent to Henry within 2 working days of receipt by the office, and Henry will assess whether there are compelling legitimate grounds to continue processing which override the interests, rights and freedoms of the individuals, or whether the information is required for the establishment, exercise or defence of legal proceedings.

10.4. Henry shall be responsible for notifying the individual of the outcome of their assessment within 10 working days of receipt of the objection.

Right to rectification

10.5. An individual has the right to request the rectification of inaccurate data without undue delay. Where any request for rectification is received, it should be sent to Henry within 2 working days of receipt by the office, and where adequate proof of inaccuracy is given, the data shall be amended as soon as reasonably practicable, and the individual notified.

10.6. Where there is a dispute as to the accuracy of the data, the request and reasons for refusal shall be noted alongside the data and communicated to the individual. The individual shall be given the option of a review under the school's complaints procedure, or an appeal direct to the Information Commissioner.

10.7. An individual also has a right to have incomplete information completed by providing the missing data, and any information submitted in this way shall be updated without undue delay.

Right to erasure

10.8. Individuals have a right, in certain circumstances, to have data permanently erased without undue delay. This right arises in the following circumstances:

10.8.1. where the personal data is no longer necessary for the purpose or purposes for which it was collected and processed.

10.8.2. where consent is withdrawn and there is no other legal basis for the processing.

10.8.3. where an objection has been raised under the right to object and found to be legitimate.

10.8.4. where personal data is being unlawfully processed (usually where one of the conditions for processing cannot be met).

10.8.5. where there is a legal obligation on the School to delete.

10.9. Henry will make a decision regarding any application for erasure of personal data and will balance the request against the exemptions provided for in the law. Where a decision is made to erase the data, and this data has been passed to other data controllers, and/or has

been made public, reasonable attempts to inform those controllers of the request shall be made.

Right to restrict processing

10.10. In the following circumstances, processing of an individual's personal data may be restricted:

10.10.1. where the accuracy of data has been contested, during the period when the School is attempting to verify the accuracy of the data;

10.10.2. where processing has been found to be unlawful, and the individual has asked that there be a restriction on processing rather than erasure.

10.10.3. where data would normally be deleted, but the individual has requested that their information be kept for the purpose of the establishment, exercise or defence of a legal claim.

10.10.4. where there has been an objection made under paragraph 10.2 above, pending the outcome of any decision.

Right to portability

10.11. If an individual wants to send their personal data to another organisation, they have a right to request that the School provides their information in a structured, commonly used, and machine-readable format. As this right is limited to situations where the School is processing the information on the basis of consent or performance of a contract, the situations in which this right can be exercised will be quite limited. If a request for this is made, it should be forwarded to Henry within 2 working days of receipt by the office.

11 Breach of any Requirement of the GDPR

11.1 Any and all breaches of the GDPR, including a breach of any of the data protection principles shall be reported as soon as discovered, to Henry.

11.2 Once notified, Henry shall assess:

11.2.1 the extent of the breach.

11.2.2 the risks to the data subject(s) as a consequence of the breach.

11.2.3 any security measures in place that will protect the information.

11.2.4 any measures that can be taken immediately to mitigate the risk to the individual(s).

11.3 Unless Henry concludes that there is unlikely to be any risk to individuals from the breach, the Information Commissioner's Office must be notified to within 72 hours of the breach having come to the attention of the School, unless a delay can be justified.

11.4 The Information Commissioner shall be told:

11.4.1 details of the breach, including the volume of data at risk, and the number and categories of data subjects.

11.4.2 the contact point for any enquiries (which shall usually be Henry).

11.4.3 the likely consequences of the breach.

11.4.4 measures proposed or already taken to address the breach.

11.5 If the breach is likely to result in a high risk to the rights and freedoms of the affected individuals then the school office shall notify data subjects of the breach without undue delay unless the data would be unintelligible to those not authorised to access it, or measures have been taken to mitigate any risk to the affected individuals.

11.6 Data subjects shall be informed of:

11.6.1 the nature of the breach.

11.6.2 who to contact with any questions.

11.6.3 measures taken to mitigate any risks.

11.7 Henry shall then be responsible for instigating an investigation into the breach, including how it happened, and whether it could have been prevented. Any recommendations for further training or a change in procedure shall be reviewed by the management and a decision made about implementation of those recommendations.

12 Contact

If anyone has any concerns or questions in relation to this policy, they should contact the school's office.

13 Note:

The school's ICO number is: Z1743933

Expiry date: July 1, 2026. Renewed annually.

Contact ICO at https://oco.org.uk/

To be reviewed annually

SAD22

Document history:

Created May 2018 / Reviewed May 2019 / Amended May 2020 / Updated May 2022
Reviewed and amended October 2024 / Reviewed and amended January 2026