Hampton Court House

# Data Protection and Privacy Policy - inc CCTV

Last Reviewed: Jan 2024
Next Review: Jan 2025

Hampton Court House

## Contents

# Data Protection and Privacy Policy

## Statement of Intent

1. Hampton Court House and Hampton Court House DayCare (hereafter referred to as HCH or our school) aims to ensure that all personal data collected about staff, students, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the Data Protection Act 2018 (DPA 2018) and General Data Protection Regulation (GDPR).

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

## Legislation and guidance

3. This policy meets the requirements 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.

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

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

## Definitions

| Term | Definition |
|---|---|
| **Personal data** | Any information relating to an identified, or identifiable, individual.<br>This may include the individual's:<br>• Name (including initials)<br>• Identification number<br>• Location data<br>• Online identifier, such as a username<br>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:<br>• Racial or ethnic origin<br>• Political opinions<br>• Religious or philosophical beliefs<br>• Trade union membership<br>• Genetics<br>• Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes<br>• Health – physical or mental<br>• 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.<br>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. |

## The data controller

6. Our school processes personal data relating to parents, students, staff, governors, visitors and others, and therefore is a data controller.

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

## Roles and responsibilities

8. 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.

### Governing board

9. The governing board has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

### Chief privacy officer - safeguarding lead

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

11. The CPO will provide an annual report of their activities directly to the governing board and, where relevant, report to the board their advice and recommendations on school data protection issues.

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

13. Full details of the CPO's responsibilities are set out in their job description.
14. Our CPO is Andy Mirza and is contactable by email on ami@hchnet.co.uk; by telephone on +44 (0)20 8943 0889 or by post at Hampton Court House, Hampton Court Road, KT8 9BS.

### Head

15. The Head acts as the representative of the data controller on a day-to-day basis.

### All staff

16. Staff are responsible for:
    a. Collecting, storing and processing any personal data in accordance with this policy
    b. Informing the school of any changes to their personal data, such as a change of address
    c. Contacting the CPO in the following circumstances:
        i. With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
        ii. If they have any concerns that this policy is not being followed
        iii. If they are unsure whether or not they have a lawful basis to use personal data in a particular way
        iv. 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
        v. If there has been a data breach
        vi. Whenever they are engaging in a new activity that may affect the privacy rights of individuals
        vii. If they need help with any contracts or sharing personal data with third parties

## Data protection principles

17. The DPA and GDPR are based on data protection principles with which the school must comply.

18. The principles say that personal data must be:
    a. Processed lawfully, fairly and in a transparent manner
    b. Collected for specified, explicit and legitimate purposes
    c. Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
    d. Accurate and, where necessary, kept up-to-date
    e. Kept for no longer than is necessary for the purposes for which it is processed
    f. Processed in a way that ensures it is appropriately secure

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

## Collecting personal data

## Lawfulness, fairness and transparency

20. We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:
    a. 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.
    b. The data needs to be processed so that the school can **comply with a legal obligation.**
    c. The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life.
    d. The data needs to be processed so that the school can perform a task **in the public interest**.
    e. 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).
    f. The individual (or their parent/carer when appropriate in the case of a student) has freely given clear **consent**.

21. 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.

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

## Limitation, minimisation and accuracy

23. 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.

24. If we want to use 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.

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

26. When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised.

## Sharing personal data

27. We will not normally share personal data with anyone else, but may do so where:
    a. There is an issue with a student or parent/carer that puts the safety of our staff or students at risk
    b. We need to liaise with other agencies – we will seek consent as necessary before doing this
    c. Our suppliers or contractors need data to enable us to provide services to our staff and students – for example, IT companies. When doing this, we will:
        i. Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
        ii. 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

iii. 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.

28. We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:
    a. The prevention or detection of crime and/or fraud
    b. The apprehension or prosecution of offenders
    c. The assessment or collection of tax owed to HMRC
    d. In connection with legal proceedings
    e. Where the disclosure is required to satisfy our safeguarding obligations
    f. Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

29. 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 students or staff.

30. 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.

## Subject access requests and other rights of individuals

### Subject access requests

31. Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them. This includes:
    a. Confirmation that their personal data is being processed
    b. Access to a copy of the data
    c. The purposes of the data processing
    d. The categories of personal data concerned
    e. With whom the data has been, or will be, shared
    f. How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
    g. The source of the data, if not the individual
    h. Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

32. Subject access requests must be submitted in writing, either by letter or email to the CPO. They should include:
    a. Name of individual
    b. Correspondence address
    c. Contact number and email address
    d. Details of the information requested

33. If staff receive a subject access request they must immediately forward it to the CPO.

### Children and subject access requests

34. 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.

35. 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, subject access requests from parents or carers of students at our school may not be granted in many cases without the express permission of the student. This is not a rule and a student's ability to understand their rights will always be judged on a case-by-case basis.

## Responding to subject access requests

36. When responding to requests, we:
    a. May ask the individual to provide 2 forms of identification
    b. May contact the individual via phone to confirm the request was made
    c. Will respond without delay and within 1 month of receipt of the request
    d. Will provide the information free of charge
    e. 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

37. We will not disclose information if it:
    a. Might cause serious harm to the physical or mental health of the student or another individual
    b. 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
    c. Is contained in adoption or parental order records
    d. Is given to a court in proceedings concerning the child

38. 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.

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

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

## Other data protection rights of the individual

41. 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:
    a. Withdraw their consent to processing at any time
    b. Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
    c. Prevent use of their personal data for direct marketing
    d. Challenge processing which has been justified on the basis of public interest
    e. Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
    f. Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
    g. Prevent processing that is likely to cause damage or distress
    h. Be notified of a data breach in certain circumstances
    i. Make a complaint to the ICO

j. Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

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

## Biometric recognition systems

43. If and when we use students' biometric data as part of an automated biometric recognition system (for example, students use fingerprints to receive school dinners instead of paying with cash), we will comply with the requirements of the Protection of Freedoms Act 2012.

44. Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The school will get written consent from at least one parent or carer before we take any biometric data from their child and first process it.

45. Parents/carers and students have the right to choose not to use the school's biometric system(s). We will provide alternative means of accessing the relevant services for those students.

46. Parents/carers and students can object to participation in the school's biometric recognition system(s), or withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

47. As required by law, if a student refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the student's parent(s)/carer(s).

48. Where staff members or other adults use the school's biometric system(s), we will also obtain their consent before they first take part in it, and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the school will delete any relevant data already captured.

## CCTV

49. We use CCTV in various locations around the school site to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV.

50. We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

51. Any enquiries about the CCTV system should be directed to Holker support or Andy Mirza.

52. Any school that employs surveillance CCTV for whatever purposes on its campus must comply with all statutory regulations covering its use, as enshrined in the Data Protection Act 1998, the Human Rights Act 1998 and in certain circumstances, the Regulation of Investigatory Powers Act 2000. There are specific requirements that refer chiefly, but not exhaustively, to the installation of CCTV equipment and its employment, as well to the collection, analysis, dissemination and storage of data collected, that the school must address and be seen to be implementing actively.

53. The CPO oversees and control all aspects of the use of surveillance CCTV and data collected from it. Registration for the use of CCTV surveillance must be maintained with the Office of the Information Commissioner, from where a suitable code of practice on its use can also be obtained.

54. An impact assessment can be a very useful method of detailing important aspects of the use of surveillance CCTV in a school and how it will affect those present, in particular, but not exclusively, staff and students. The impact assessment needs to address the following requirements.

55. The exact purpose for the use of surveillance CCTV in each any every area of coverage.

56. An assessment of the suitability for the use of CCTV over other methods considered for achieving the same or similar outcome.

57. An assessment of the proportionality of the level of coverage employed, with regard to amount of equipment in use and time periods for which it is activated

58. The possible/potential ways in which the data collected could be used, affecting directly or indirectly those monitored, including any restrictions on its usage, for each and every area of coverage.

59. Where any/all data is stored for later possible use, the suitability of this over other methods to achieve the same information and outcomes.

60. For each and every area of coverage, the identification of personnel having immediate access to the data collected through general authorisation as part of their specific duties, including the data controlling officer and other systems' monitors with general or limited authorisation on their behalf to view the data for whatever purpose.

61. For each and every area of coverage, where data may be stored, how and by whom the data will be processed in any manner, and for what purpose.

62. For each and every area of coverage, the identification of personnel who can gain access to any/all data collected, as an intrinsic part of their duties (only if requisite authorisation has been granted, permanently or temporarily) and where possible, indication of whether any authorised use can be made of the released data, as well as any restrictions placed upon its use by the third party.

63. Detailed methods by which all personnel, whose images could be captured by an active surveillance CCTV system, will be informed of this possibility, including appropriate signs and channels through which further information can be obtained.

64. Specifically, in addition to the above, if the CCTV surveillance equipment is entirely operated by an outside agency, which also controls the collection, monitoring and use of to this effect with full contact details of the agency.

65. perform in their most effective and personally comfortable way; this including both staff and students, but not exclusively. Whilst this assessment is bound to have a significant subjective element, it should nevertheless be considered as an important part of the overall statement.

| CAMERA AREA | No. | | CAMERA AREA | No. |
|---|---|---|---|---|
| Art room | 2 | | G5 classroom | 1 |
| Outside art room | 1 | | Back gate | 1 |
| Gallery main hall | 1 | | Security Guard cabin inside | 1 |
| Conservatory stairs | 1 | | Main gates – outside cabin near floodlights | 1 |
| Little garden wall | 1 | | Pedestrian gate – on the post near front gate wall | 1 |
| Drive along perimeter wall | 1 | | Main Car park – on the post front gate wall | 1 |
| Main hall | 1 | | ICT corridor | 1 |
| Kitchen | 1 | | S Block outside S1 & 2 | 1 |
| S2 classroom inside | 1 | | Stairs between hall and G2 corridor | 1 |
| Theatre | 1 | | Outside lavatory, Lab 1 & 2 | 1 |

Purpose(s) for use of surveillance CCTV:

- To provide a safe and secure environment for pupils, staff and visitors.
- To protect the school buildings and assets
- To assist in reducing the fear of crime and for the protection of the private property.
- To provide a deterrent effect and assist law enforcements agencies in apprehending offenders.
- To assist in traffic managements and car parking schemes.

The system is cloud based and accessible via: Live View | UNVR (ui.com)

## Photographs and videos

66. As part of our school activities, we may take photographs and record images of individuals within our school.
67. We will obtain written consent from parents/carers, or students aged 18 and over, for photographs and videos to be taken of students for communication, marketing and promotional materials.
68. Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and student. Where we don't need parental consent, we will clearly explain to the student how the photograph and/or video will be used.

69. Uses may include:
    a. Within school on notice boards and in school magazines, brochures, newsletters, etc.
    b. Outside of school by external agencies such as the school photographer, newspapers, campaigns
    c. Online on our school website or social media pages

70. 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.

71. 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.

## Data protection by design and default

72. We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:
    a. Appointing a suitable CPO, and ensuring they have the necessary resources to fulfil their duties.
    b. 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.
    c. Completing privacy 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 CPO will advise on this process).
    d. Integrating data protection into internal documents including this policy, any related policies and privacy notices.
    e. 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.
    f. Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant.
    g. Maintaining records of our processing activities, including:
        i. For the benefit of data subjects, making available the name and contact details of our school and CPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
        ii. 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

## Data security and storage of records

73. 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.

74. In particular:
    a. Paper-based records and portable electronic devices, such as laptops and hard drives that contain unencrypted personal data are kept under lock and key when not in use.

b. 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
c. Where personal information needs to be taken off site, staff must sign it in and out from the school office
d. 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 students are reminded to change their passwords at regular intervals
e. Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
f. Staff, students 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 ICT policy and acceptable use agreement).
g. 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 Sharing personal data).

## Disposal of records

75. 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.

76. 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.

## Personal data breaches

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

78. In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1.

79. When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a school context may include, but are not limited to:
    a. A non-anonymised dataset being published on the school website which shows the exam results of students.
    b. Safeguarding information being made available to an unauthorised person
    c. The theft of a school laptop containing non-encrypted personal data about students

## Training

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

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

## Monitoring arrangements

82. The CPO is responsible for monitoring and reviewing this policy, subject to approval by the governing body.

83. This policy will be reviewed every 2 years or more frequently should a change in the law, guidance, or our practice necessitate any change to this policy.

## Links with other policies

84. This data protection policy is linked to our:
    a. Privacy Notice
    b. Staff Code of Conduct
    c. Safeguarding and Child Protection Policy and Procedures
    d. ICT Acceptable Use Policy

## Appendix 1: Personal data breach procedure

85. This procedure is based on guidance on personal data breaches produced by the ICO.

86. On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the CPO

87. The CPO will investigate the report, and determine whether a breach has occurred. To decide, the CPO will consider whether personal data has been accidentally or unlawfully:
    a. Lost
    b. Stolen
    c. Destroyed
    d. Altered
    e. Disclosed or made available where it should not have been
    f. Made available to unauthorised people

88. The CPO will alert the  and the chair of governors

89. The CPO 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)

90. The CPO will assess the potential consequences, based on how serious they are, and how likely they are to happen

91. The CPO 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 CPO 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:
    a. Loss of control over their data
    b. Discrimination
    c. Identify theft or fraud
    d. Financial loss
    e. Unauthorised reversal of pseudonymisation (for example, key-coding)
    f. Damage to reputation
    g. Loss of confidentiality
    h. Any other significant economic or social disadvantage to the individual(s) concerned

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

93. The CPO 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 the school's computer system.

94. Where the ICO must be notified, the CPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the CPO will set out:
    a. A description of the nature of the personal data breach including, where possible:
        i. The categories and approximate number of individuals concerned
        ii. The categories and approximate number of personal data records concerned
    b. The name and contact details of the CPO
    c. A description of the likely consequences of the personal data breach

d. 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

95. If all the above details are not yet known, the CPO will report as much as they can within 72 hours.

96. The report will explain that there is a delay, the reasons why, and when the CPO expects to have further information. The CPO will submit the remaining information as soon as possible

97. The CPO 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 CPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
    a. The name and contact details of the CPO
    b. A description of the likely consequences of the personal data breach
    c. 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

98. The CPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies

99. The CPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    a. Facts and cause
    b. Effects
    c. Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

100. Records of all breaches will be stored on the school's computer system.

101. The CPO and Head 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

102. 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)

103. 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

104. Members of staff who receive personal data sent in error must alert the sender and the CPO as soon as they become aware of the error

105. If the sender is unavailable or cannot recall the email for any reason, the CPO will ask the ICT department to recall it

106. In any cases where the recall 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

107. The CPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request

108. The CPO 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.