The Tiffin Girls' School

DATA PROTECTION POLICY

REVISED MARCH 2026

INTRODUCTION

1. Everyone has rights with regard to the way in which their personal data is handled. The Tiffin Girls' School (the School) acknowledges that during the course of our activities we will collect, store and process personal data about staff, students, parents and others. This means the School is a data controller in relation to that personal data. The School is registered as a data controller with the Information Commissioner's Office (ICO) and will renew this registration annually or as otherwise legally required.

2. The School is also obliged to collect, store and process personal data to fulfil our obligations to the local authority, Department for Education and other bodies.

3. The personal data held by the School is subject to certain legal safeguards specified in the UK General Data Protection Regulation (GDPR), the Data Protection Act 2018 (DPA 2018), the Data Use and Access Act 2025 and other regulations (together 'Data Protection Legislation').

4. The School is committed to the protection of all personal data and special category personal data for which we are the data controller. We deal with information properly in whatever way it is collected, recorded and used – on paper, electronically, in the 'cloud' or any other way. We regard the lawful and correct treatment of personal information as very important to successful operations and to maintaining confidence between those with whom we deal and ourselves. We are conscious that much of the data we hold is classified as sensitive personal data and we are aware of the extra care this kind of information requires.

5. This policy and other documents referred to in it set out the basis on which the School will process any personal data collected from data subjects, or that is provided to us by data subjects or other sources.

6. This policy should be read in conjunction with the following school policies:

- Practical Guidance for Staff on Data Protection
- Records Management
- Records Retention Scheme
- Online Safety
- Freedom of Information Publication Scheme
- Artificial Intelligence
- CCTV
- Photographs and Images
- ICT Acceptable Usage Agreements

7. All staff have a role to play in the School's data protection compliance and must comply with this policy when processing data on behalf of the School. Any breach of this policy may result in disciplinary or other action.

8. Any references to staff in this policy include peripatetic staff, volunteers, governors and members of the academy trust.

9. Definitions of terms used in this policy can be found in Appendix 1.

COMPLIANCE MEASURES

10. The School helps to ensure compliance with Data Protection Legislation using the measures outlined below.

Training

11. All school employees receive data protection training as part of their induction and refresher training is provided annually.

12. The training includes (but is not limited to) the practical application of data protection principles in a school context, guidance on how to keep personal data secure and when staff should contact the Data Protection Officer.

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

14. Staff are encouraged to ask questions and raise concerns with the Data Protection Officer. This allows the School to regularly review and strengthen the data protection measures that are in place.

Documentation

15. Documenting how we comply with data protection law is a key part of our compliance. In addition to the documents listed in paragraph 6, we:

- maintain a record of how we use personal data as required under Article 30 of the GDPR
- document our lawful bases for using personal data through our privacy notices
- keep a record of our legitimate interests' assessments
- carry out risk assessments and, when required, a data protection impact assessment
- retain records of any consents obtained to use personal data
- maintain a register of any data breaches. The Data Protection Officer is responsible for maintaining this. All staff understand that they must inform the Data Protection Officer of any suspected breach so that the register can be kept up to date
- record when staff complete data protection training

Privacy Notices

16. The School has provided privacy notices to the individuals whose personal data we process. These privacy notices are published on the School's website.

17. We are mindful that our students are competent to exercise their own data protection rights. In light of this, we have developed a privacy notice for students that is age appropriate and addressed directly to the students.

18. In addition, the School explains how personal data will be used on a case-by-case basis as appropriate. For example, forms that are used to collect personal data will include a brief description of how and why it will be used, and cross-refer to the applicable privacy notice on our website.

Data Protection by Design and Default

19. The School has built the data protection principles into practices by implementing appropriate technical and organisational measures. This is known as data protection by design.

20. We also ensure that we only use the minimum amount of personal data to achieve our purposes. This is known as data protection by default.

21. More specifically, we do the following:

- Ensure the Data Protection Officer has the necessary resources to fulfil their duties and maintain their expert knowledge
- Only process 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
- Complete data protection impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies
- Integrate data protection into internal documents, any related policies and privacy notices
- Conduct reviews and audits to test our privacy measures and make sure we are compliant

ROLES AND RESPONSIBILITIES

Governing Board

22. The Governing Board has overall responsibility for ensuring that the School complies with all relevant data protection obligations.

Data Protection Officer

23. The Data Protection Officer (DPO) is responsible for overseeing the implementation of this policy, monitoring the School's compliance with data protection law, and developing related policies and guidelines where applicable.

24. They 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.

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

26. The School's DPO is Emma Kilburn, Senior Deputy Headteacher, and is contactable via dataprotection@tiffingirls.org

Headteacher

27. The Headteacher acts as the representative of the data controller on a day-to-day basis.

All staff

28. Staff are responsible for:
- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address
- Contacting the DPO in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - If they have any concerns that this policy is not being followed
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the UK
    - If there has been a data breach
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
    - If they need help with any contracts or sharing personal data with third parties

DATA PROTECTION PRINCIPLES

29. Anyone processing personal data must comply with the data protection principles of lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage minimisation, integrity and confidentiality (security) and accountability. Specifically, personal data must be:

- Processed lawfully, fairly and in a transparent manner in relation to the data subject
- Processed for specified, lawful purposes and in a way that is not incompatible with those purposes
- Adequate, relevant and not excessive for the purpose
- Accurate and up to date
- Kept for no longer than is necessary for the purpose
- Processed securely using appropriate technical and organisational measures

30. Personal data must also:

- Be processed in line with data subjects' rights
- Not be transferred to people or organisations situated in other countries without adequate protection

31. The School shall be responsible for, and be able to demonstrate compliance with, paragraphs 29 and 30 above.

COLLECTING PERSONAL DATA

Fair and Lawful Processing

32. Data Protection Legislation is not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject.

33. For personal data to be processed fairly, data subjects must be made aware:

- that the personal data is being processed
- why the personal data is being processed
- what the lawful basis is for that processing (see below)
- whether the personal data will be shared, and if so with whom
- the period for which the personal data will be held
- the existence of the data subject's rights in relation to the processing of that personal data
- the right of the data subject to raise a complaint with the School in relation to any processing (see paragraphs 118-120 below)

34. For personal data to be processed lawfully, it must be processed on the basis of one of the legal grounds set out in the Data Protection Legislation. The School will normally process personal data under the following legal grounds:

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

35. When special category personal data is being processed, an additional legal ground must apply to that processing. The School normally only processes special category data under the following legal grounds:

- the individual (or their parent/carer when appropriate in the case of a student) has given explicit consent
- the data needs to be processed to perform or exercise obligations or rights in relation to employment, social security or social protection law
- the data needs to be processed to ensure the vital interests of the individual or another person, where the individual is physically or legally incapable of giving consent
- the data has already been made manifestly public by the individual
- the data needs to be processed for the establishment, exercise or defence of legal claims
- the data needs to be processed for reasons of substantial public interest as defined in legislation
- the data needs to be processed for health or social care purposes, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law
- the data needs to be processed for public health reasons, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law
- the data needs to be processed for archiving purposes, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest

36. For criminal offence data, we will meet both a lawful basis and a condition set out under data protection law. Conditions include:

- The individual (or their parent/carer when appropriate in the case of a student) has given consent
- The data needs to be processed to ensure the vital interests of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made manifestly public by the individual
- The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of legal rights
- The data needs to be processed for reasons of substantial public interest as defined in legislation

37. The School processes criminal offence data in storing the outcome of a Disclosure and Barring Service (DBS)check on employees, non-employed staff and volunteers. As this data relates to criminal convictions, collecting and retaining it means the School is processing criminal offence data. This applies even though the check has not revealed any conviction.

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

39. If any data user is in doubt as to whether they can use any personal data for any purpose, then they must contact the DPO before doing so.

40. We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect, or use personal data in ways that have unjustified adverse effects on them.

Vital Interests

41. There may be circumstances in which it is considered necessary to process personal data or special category personal data in order to protect the vital interests of a data subject. This might include medical emergencies where the data subject is not in a position to give consent to the processing. We believe that this will only occur in very specific and limited circumstances. In such circumstances, we would usually seek to consult with the DPO in advance, although there may be emergency situations where this does not occur.

Consent

42. Where none of the other bases for processing set out above apply then the School must seek the consent of the data subject before processing any personal data for any purpose.

43. There are strict legal requirements in relation to the form of consent that must be obtained from data subjects.

44. When students and staff join the School, a consent form will need to be completed in relation to them. This consent form deals with the taking and use of photographs and videos of them, amongst other things. Where appropriate third parties may also be required to complete a consent form.

45. In relation to all students under the age of 13 years old, we will seek consent from an individual with parental responsibility for that student.

46. We will generally seek consent directly from a student who has reached the age of 13. However, we recognise that this may not be appropriate in certain circumstances and therefore may be required to seek consent from an individual with parental responsibility.

47. If consent is required for any other processing of personal data of any data subject, then the form of this consent must:

- Inform the data subject of exactly what we intend to do with their personal data
- Require them to positively confirm that they consent – we cannot ask them to opt-out rather than opt-in
- Inform the data subject of how they can withdraw their consent.

48. Any consent must be freely given, which means that we cannot make the provision of any goods or services or other matter conditional on a data subject giving their consent.

49. The DPO must always be consulted in relation to any consent form before consent is obtained.

50. A record must always be kept of any consent, including how it was obtained and when.

Limitation, minimisation and accuracy

51. 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.

52. 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.

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

54. We will keep data accurate and, where necessary, up-to-date. We will take reasonable steps to destroy or amend inaccurate or out-of-date data.

55. When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the school's Records Retention Schedule.

SHARING PERSONAL DATA

56. We will not normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. These include, but are not limited to, situations where:

- There is an issue with a student or parent/carer that puts the safety of our staff at risk
- We need to liaise with other organisations. Such organisations include:
  - Department for Education
  - Ofsted
  - Health authorities and professionals
  - The local authority
  - Examination bodies
  - Other schools
- 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:
  - Only appoint suppliers or contractors who can provide sufficient guarantees that they comply with data protection law
  - Establish a data processing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
  - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

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

58. 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.

59. Where we transfer personal data internationally, we will do so in accordance with data protection law.

SUBJECT ACCESS REQUESTS AND OTHER RIGHTS OF INDIVIDUALS

Subject access requests

60. Individuals have a right to make a 'subject access request' to gain access to personal information that the School holds about them. This includes:
- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual
- Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing
- the right of the data subject to raise a complaint with the School in relation to a subject access request (see paragraphs 118-120 below).
- The safeguards provided if the data is being transferred internationally

61. Subject access requests can be submitted in any form, including verbal, but we may be able to respond to requests more quickly if they are made in writing and include:

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

62. If staff receive a subject access request in any form, including verbal, they must immediately forward it to the DPO.

63. The DPO coordinates the School's response to all subject access requests and will involve other members of staff as appropriate.

Children and subject access requests

64. 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.

65. Children aged 13 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of students at our school may not be granted 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

66. When responding to requests, we:

- May ask the individual to provide two forms of identification, one of which should be photo ID
- May contact the individual via phone to confirm the request was made
- May ask the individual to clarify what information they need if the request is non-specific as this may enable a quicker response
- Will respond without delay and within one month of receipt of the request (or receipt of the additional information needed to confirm identity, where relevant)
- Will provide the information free of charge
- May tell the individual we will comply within three months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within one month, and explain why the extension is necessary. In particular, this may apply if a request is submitted during the summer holidays and multiple staff are required to source the data.

67. We may not disclose information for a variety of reasons, such as if it:

- Might cause serious harm to the physical or mental health of the student or another individual
- Would reveal that the child is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Would include another person's personal data that we can't reasonably anonymise, and we don't have the other person's consent and it would be unreasonable to proceed without it
- Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts

68. If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee to cover administrative costs. We will take into account whether the request is repetitive in nature when making this decision.

69. 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

70. 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, individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Object to processing which has been justified on the basis of public interest, official authority or legitimate interests
- Challenge decisions based solely on automated decision making or profiling (i.e. making decisions or evaluation certain things about an individual based on their personal data with no human involvement)
- Be notified of a data breach (in certain circumstances)
- Make a complaint to the School (see paragraphs 118-120 below)
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

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

<u>The Right to Object</u>

72. In certain circumstances data subjects may object to us processing their personal data. This right may be exercised in relation to processing that we are undertaking on the basis of a legitimate interest or in pursuit of a statutory function or task carried out in the public interest.

73. An objection to processing does not have to be complied with where the School can demonstrate compelling legitimate grounds that override the rights of the data subject.

74. In respect of direct marketing, any objection to processing must be complied with.

75. The School is not however obliged to comply with a request where the personal data is required in relation to any claim or legal proceedings.

<u>The Right to Rectification</u>

76. If a data subject informs the School that personal data held about them by the School is inaccurate or incomplete, then we will consider that request and provide a response within one month.

77. If we consider the issue to be too complex to resolve within that period, then we may extend the response period by a further two months. If this is necessary, then we will inform the data subject within one month of the request that this is the case.

78. We may determine that any changes proposed by the data subject should not be made. If this is the case, then we will explain to the data subject why this is the case. In those circumstances we will inform the data subject of the right to complain to the Information Commissioner's Office at the time that we inform them of our decision in relation to their request.

The Right to Restrict Processing

79. Data subjects have a right to "block" or suppress the processing of personal data. This means that the School can continue to hold the personal data but not do anything else with it.

80. The School must restrict the processing of personal data:

- Where it is in the process of considering a request for personal data to be rectified (see above)
- Where the School is in the process of considering an objection to processing by a data subject
- Where the processing is unlawful but the data subject has asked the School not to delete the personal data
- Where the School no longer needs the personal data but the data subject has asked the School not to delete the personal data because they need it in relation to a legal claim, including any potential claim against the School.

81. If the School has shared the relevant personal data with any other organisation then we will contact those organisations to inform them of any restriction, unless this proves impossible or involves a disproportionate effort.

The Right to Be Forgotten

82. Data subjects have a right to have personal data about them held by the School erased only in the following circumstances:

- Where the personal data is no longer necessary for the purpose for which it was originally collected
- When a data subject withdraws consent – which will apply only where the School is relying on the individuals consent to the processing in the first place
- When a data subject objects to the processing and there is no overriding legitimate interest to continue that processing – see above in relation to the right to object
- Where the processing of the personal data is otherwise unlawful
- When it is necessary to erase the personal data to comply with a legal obligation.

83. The School is not required to comply with a request by a data subject to erase personal data if the processing is taking place:

- To exercise the right of freedom of expression or information
- To comply with a legal obligation for the performance of a task in the public interest or in accordance with the law
- For public health purposes in the public interest
- For archiving purposes in the public interest, research or statistical purposes
- In relation to a legal claim.

84. If the School has shared the relevant personal data with any other organisation then we will contact those organisations to inform them of any erasure, unless this proves impossible or involves a disproportionate effort.

Right to Data Portability

85. In limited circumstances, a data subject has a right to receive their personal data in a machine-readable format, and to have this transferred to other organisations.

PARENTAL REQUESTS TO SEE THE EDUCATIONAL RECORD

86. As the School is an academy trust, there is no automatic parental right of access to the educational record of their child. However, parents may submit a request by emailing dataprotection@tiffingirls.org and the school will endeavour to respond within 15 school days. The response will only include records held by the school that are not already available via the parent portal.

ARTIFICIAL INTELLIGENCE

87. Artificial intelligence (AI) tools are now widespread and easy to access. The School recognises that AI has many uses to help students learn, but also poses risks to sensitive and personal data.

88. To ensure that personal and sensitive data remains secure, staff are not permitted to enter such data relating to students, staff or parents into generative AI tools or chatbots.

89. If personal and/or sensitive data is entered into an generative AI tool, the School will treat this as a data breach, and will follow the personal data breach procedure outlined in appendix 2.

90. Further information and guidance regarding how the School uses AI tools can be found in the School's Artificial Intelligence Policy.

BIOMETRIC DATA

91. The School does not have any biometric recognition systems installed and therefore does not collect any biometric data such as fingerprints or facial recognition information (retina and iris patterns).

CCTV

92. 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.

93. 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.

94. Further information can be found in the School's CCTV Policy and any enquiries about the CCTV system should be directed to the DPO.

PHOTOGRAPHS AND VIDEOS

95. During a student's time at the School, images (including still photography and video) will be taken of activities which involve students. The photographs may be used for all usual School purposes, including displays (digital and conventional notice boards), school publications, advertising and marketing, on the School website, the Schools' social media presence (for example Bluesky, Instagram and LinkedIn), and in year books .

96. When using photographs and videos in this way we will not accompany them with any personal information that would allow students to be identified.

97. Certain uses of images are necessary for the ordinary running of the School, including for important safeguarding purposes such as identification and security. The legal basis for this is public task as the School is exercising its legal duties to safeguarding students. All students are photographed on entering the school at Year 7 and at the start of Year 10 and Year 12 for the purposes of internal identification.

98. Consent is required for photographs of students to be shared on the School's social media channels, website or elsewhere online, for example, the alumnae website.

99. Consent is required for other uses of images in, for example, communication, marketing and promotional materials. This may include printed materials such as year books, and/or displays within the school.

100. Consent for images being used in the ways set out in paragraphs 98 and 99 above is sought in the online enrolment forms for Year 7 and Year 12 students joining the school.

101. Parents should be aware that, from the age of 13 and upwards, the law recognises students' own rights to have a say in how their personal information is used, including images.

102. Parents or students aged 13 years and over who wish to alter their consent regarding the use of images should email the Data Protection Officer at dataprotection@tiffingirls.org.

103. In most circumstances, consent for photography cannot be withdrawn retrospectively. For example, photographs of a student that have already been taken and published in print cannot be recalled if permission for photography is withdrawn after publication. For digital/online photographs, we shall, where possible, endeavour to remove photographs where consent is withdrawn.

104. Any photographs and videos taken by parents/carers at school events for their own personal use are not covered by data protection legislation. However, we request that photos or videos with other students are not shared with other adults whose children are not included in the photograph/video, including sharing via social media.

105. Further information can be found in the School's Photographs and Images Policy and any enquiries should be directed to the DPO.

CARD TERMINALS

106. The School is cashless and has two card terminals for taking payments for fundraising activities, tickets for school productions and other events.

107. The School complies with the Payment Card Industry Data Security Standard in order to protect cardholder data and reduce the risk of a data security breach.

DATA SECURITY AND STORAGE OF RECORDS

108. The School has put in place appropriate technical and organisational measures to minimise the risk of unlawful or unauthorised processing of personal data, and to minimise the risk of accidental loss of, or damage to, personal data.

109. The School has put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction.

110. The DPO is responsible for determining the appropriate organisational measures, for example, staff training and guidance.

111. The Finance Director has oversight of network security, with responsibility delegated to the IT Managed Service Provider.

112. Security measures include (but are not limited to):

- Entry controls to the school site and all buildings
- Secure lockable offices, desks and cupboards
- Shredders and locked containers for larger quantities of documents that require shredding
- Secure Wi-Fi network
- Minimum password complexity requirements

- Appropriate firewall
- Remote backup solution for network servers
- ICT acceptable usage agreements for staff, students and visitors

DISPOSAL OF RECORDS

113. 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.

114. For example, we will shred 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

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

116. In the unlikely event of a suspected data breach, we will follow the procedure set out in Appendix 2.

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

COMPLAINTS

118. Complaints regarding data protection matters can be made by emailing the DPO via dataprotection@tiffingirls.org or by telephoning the school on 020 8546 0773 and asking to speak with the DPO. Complainants should identify how they would like their complaint to be resolved.

119. The following procedure will be followed:

- Complaints will be acknowledged within 30 days of receipt
- The DPO may request photographic identification if the complaint relates to the complainant's personal data
- The DPO will conduct an investigation, without undue delay, that may include:
    - Reviewing relevant facts thoroughly, fairly and accurately
    - Seeking clarification and/or further information from the complainant if needed
    - Speaking to relevant members of staff
    - Comparing the information in the complaint with the information held by the School
    - Checking the School's policies and procedures have been followed
- The DPO will determine whether the complaint is upheld or rejected in full or in part and provide the complainant with a written response to their complaint, to include:
    - A summary of the investigation process
    - The outcome of the complaint
    - Where appropriate, any actions taken by the School

120. If the complainant is unsatisfied with the School's response, they should contact the Information Commissioner via www.ico.org

MONITORING ARRANGEMENTS

121. The DPO is responsible for monitoring and reviewing this policy on an annual basis.

APPENDIX 1: DEFINITIONS

Data	Information stored electronically, on a computer or in paper-based filing systems.
Data subject	For the purpose of this policy this includes all living individuals about whom the School holds personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information.
Personal data	Any information relating to an identified or identifiable natural person (a data subject). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as: • name (including initials) • identification number • location data • online identifier, such as a username • factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity
Data controller	A person or organisation that determines the purposes and the manner in which personal data is processed. They are responsible for establishing practices and policies in line with Data Protection Legislation.
Data user	Staff (including governors and volunteers) whose work involves processing personal data. Data users must protect the data they handle in accordance with the Data Protection Policy and any applicable data security procedures at all times.
Data processor	Any person or organisation that processes data on behalf of the School and on the School's instructions
Processing	Any activity that involves the use of personal data, including collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing also includes transferring personal data to third parties.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetic information • Biometric information (such as fingerprint, retina and iris patterns), where used for identification purposes. • Health matters (such as medical information) – physical or mental • Sexual matters or sexual orientation The DfE guidance recommends best practice treatment of the following as special category data • A safeguarding matter • Students in receipt of pupil premium

	• Students with special educational needs and disability • Children in need • Children looked after by a local authority
Data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

APPENDIX 2: Personal data breach procedure

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

a) On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO by emailing dataprotection@tiffingirls.org

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

c) Staff and governors will cooperate with the investigation (including allowing access to information and responding to questions). The investigation will not be treated as a disciplinary investigation.

d) If a breach has occurred or it is considered to be likely that is the case, the DPO will alert the Headteacher. If the breach meets the threshold for reporting to the ICO, the DPO will also inform the Chair of Governors.

e) The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. The DPO should take external advice when required (e.g. from IT providers). (Actions relevant to specific data types are set out at the end of this procedure).

f) The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen before and after the implementation of steps to mitigate the consequences.

g) The DPO will determine whether the breach should be reported to the ICO and the individuals affected by completing the ICO's self-assessment tool. The DPO will keep a record of the outcome of this process.

.

h) Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website, or through its breach report line (0303 123 1113), within 72 hours of the School's awareness of the breach. As required, the DPO will set out:
- A description of the nature of the personal data breach including, where possible:
  - The categories and approximate number of individuals concerned
  - The categories and approximate number of personal data records concerned
- The name and contact details of the DPO
- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

i) If all the above details are not yet known, the DPO will report as much as they can within 72 hours of the School's awareness of the breach. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible.

j) Where the School is required to communicate with individuals whose personal data has been breached, the DPO will tell them in writing. This notification will set out:

- A description, in clear and plain language, of the nature of the personal data breach
- The name and contact details of the DPO
- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned

k) The DPO will consider, in light of the investigation and any engagement with affected individuals, whether to notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies.

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

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

n) Depending on the seriousness of the breach, the DPO will keep the Headteacher informed throughout the process. If deemed necessary, the DPO and Headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.

o) The DPO and Headteacher will periodically assess recorded data breaches and identify any trends or patterns requiring action by the School to reduce risks for future breaches.

Actions to minimise the impact of data breaches

p) We set out below the steps we might take to try and mitigate the impact of different types of data breach if they were to occur, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error.
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error.
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to attempt to recall it from external recipients and remove it from the School's email system (retaining a copy if required as evidence).
- In any cases where the recall is unsuccessful or cannot be confirmed as successful, the DPO will consider whether it is appropriate to contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way.
- The DPO will endeavour to obtain a written response from all the individuals who received the data, confirming that they have complied with this request.
- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted.
- If safeguarding information is compromised, the DPO will inform the designated safeguarding lead and discuss whether the school should inform any, or all, of its local safeguarding partners (e.g. the local authority, police, health partners).