The Crypt School Data Protection Policy

Lead Persons: **IT Manager; Compliance Officer**
SLT Member Responsible: **Senior Deputy Head**
Governing Body Committee: Pupil Education & Outcomes

Introduction

1. During the course of its work, the School has to collect, store and process personal data about pupils and their parents, staff and volunteers, governors, suppliers and other third parties. This policy sets out how The Crypt School will implement its obligations to protect personal data under the UK General Data Protection Regulation (GDPR), the Data Protection Act 2018 and the Data (Use and Access) Act 2025. "Personal data" means data that relates to a living individual who can be identified, directly or indirectly. It includes names, addresses and other contact details, photographs, identification numbers or online identifiers and location data. “Special Category Data” is information about racial or ethnic origin, sexual life or sexual orientation, biometric and genetic data, religious beliefs (or similar), physical or mental health/condition, membership of a trade union, political opinions or beliefs, details of proceedings in connection with an offence or an alleged offence.

2. The Crypt School is committed to the protection of all personal data for which it holds responsibility as the data controller and the handling of such data in line with the data protection principles and data protection legislation. Changes to data protection legislation shall be monitored and implemented in order to remain compliant with all requirements.

3. As a recognized data controller, our data processing activities are registered with the Information Commissioner’s Office (ICO): Register of Data Controllers. The School maintains a Record of Processing Activities in accordance with Article 30 of the UK GDPR.

Scope and application

4. This policy covers:

    a. management of the life cycle of records and information containing personal data, from creation or receipt to disposal or transfer;

b. the processing of personal data by The Crypt School. "Processing" means obtaining, recording or holding the information or data or carrying out any or set of operations on the information or data.

5. The requirements of this policy are mandatory for governors, all staff employed by the School and any third party contracted to provide services within or on behalf of The Crypt School. The School is committed to ensuring that its staff are aware of data protection legal requirements and policies, and that adequate training is provided.

6. The Data Protection Act 2018 (DPA 2018) outlines the requirement for an Appropriate Policy Document (APD) to be in place when processing special category (SC) and criminal offence (CO) data under certain specified conditions.

7. This document meets the requirement at paragraph 1 of Schedule 1 to the Data Protection Act 2018 that an appropriate policy document be in place where the processing of special category personal data is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the controller or the data subject in connection with employment, social security or social protection.

8. It also meets the requirement at paragraph 5 of Schedule 1 to the Data Protection Act 2018 that an appropriate policy document be in place where the processing of special category personal data is necessary for reasons of substantial public interest. The specific conditions under which data may be processed for reasons of substantial public interest are set out at paragraphs 6 to 28 of Schedule 1 to the Data Protection Act 2018 and the School intends to rely on these as and when appropriate, with particular reliance on paragraph 18, 'Safeguarding of children and individuals at risk' and paragraph 17, 'Counselling'.

9. The **Freedom of Information Policy** covers the School's obligations in relation to the handling of information requests made to the School under the Freedom of Information Act 2000. The **Acceptable Use Policies for Pupils and for Adults** provide rules and guidance on the safe and appropriate use of IT in School and use of School IT equipment. The **Cybersecurity Policy** sets out the School's overall approach to cybersecurity and the **Secure Disposal of IT Equipment Policy** describes how the School arranges the secure disposal of redundant data and equipment.

The data protection principles

10. The UK GDPR data protection principles shall be applied to all personal data processed. They require that personal data shall be:

- processed lawfully, fairly and in a transparent manner
- collected for specified, explicit and legitimate purposes, and not further processed in a manner that is incompatible with those purposes ('purpose limitation'). This means the School must be clear about its purposes for processing personal information from the start, and must only re-use the personal information for a new purpose if this is compatible with the original purpose. For personal information collected under consent, the rules are more restrictive and may require a new consent

- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')
- accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (to maintain accuracy)
- kept in a form that permits identification for no longer than is necessary
- processed in accordance with the data subject's rights
- processed in a way that ensures appropriate security, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage.

11. As a data controller, the School must also be able to demonstrate compliance with these principles ("accountability" principle). This includes keeping evidence of the steps the School takes to comply with the UK GDPR and putting in place appropriate technical and organisational measures, such as:

- adopting and implementing data protection policies (where proportionate);
- taking a 'data protection by design and default' approach - putting appropriate data protection measures in place throughout the entire lifecycle of our processing operations;
- putting written contracts in place with organisations that process personal data on our behalf;
- maintaining documentation of our processing activities;
- implementing appropriate security measures;
- recording and, where necessary, reporting personal data breaches;
- carrying out data protection impact assessments for uses of personal data that are likely to result in high risk to individuals' interests;
- appointing a data protection officer (where necessary); and
- adhering to relevant codes of conduct and signing up to certification schemes (where possible).

Fair obtaining and processing

12. The Crypt School undertakes to obtain and process personal data fairly, lawfully and in a transparent manner, by explaining the purposes for which data are used; whom we share data with; and the rights of those whose data we hold. This information is set out in our privacy notices, which are available on the School's website and circulated to pupils, parents (i.e. any person having parental responsibility or care of a child) and all people working at the School.

13. If we offer online services to pupils, such as classroom apps, we intend to rely on Public Task as a basis for processing; where this is not appropriate, we will get parental consent for processing (except for online counselling and preventive services).

14. There are circumstances where the School is required either by law or in the best interests of our students or staff to pass information on to external authorities: for example, health authorities, local authorities, examination authorities, the police and courts and the

Department for Education. If a pupil transfers from The Crypt School to another school, their records and other data that relates to their health and welfare will be forwarded on to the new school to support a smooth transition. Information on data sharing is set out in our privacy notices.

15. Where the School uses other organisations to process data on its behalf, it will ensure that these processors can provide sufficient guarantees that the requirements of data protection legislation will be met and the rights of data subjects protected, and that a written contract is in place including the terms and details required by the UK GDPR.

16. Changes to the type of data processing activities being undertaken shall be notified to the ICO and details amended in the register.

Limitation, Minimisation and Accuracy

17. The School 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.

18. 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.

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

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

International transfers of data

21. Individuals risk losing the protection of UK data protection law if their personal information is sent (or made accessible) outside the UK. The UK GDPR therefore contains rules about transfers of personal information to separate organisations located outside the UK. The School complies with these requirements and staff who are considering an international transfer of personal data should consult the School's Compliance Officer and Data Protection Officer for advice.

Processing of special categories of personal data and criminal offence data

22. As part of our statutory functions, we process special category data and criminal offence data in accordance with the requirements of Articles 9 and 10 of the General Data Protection Regulation (UK GDPR') and Schedule 1 of the Data Protection Act 2018 ('DPA 2018'). Article 10 of the UK GDPR covers processing in relation to criminal convictions and offences or related security measures. In addition, section 11(2) of the DPA 2018 specifically confirms that this includes personal data relating to the alleged commission of offences or proceedings for an offence committed or alleged to have been committed, including sentencing. This is collectively referred to as 'criminal offence data'.

Consent to process personal data

23. For a small number of activities, the School requires the consent of individuals to process their personal data. Where this is the case, we ensure that:

    a. distinct consent is sought for different processing operations;
    b. consent is given in a clear, affirmative way;
    c. consent is not a precondition for participating fully in School activities;
    d. clear records are kept;
    e. people are given information on how to exercise their right to withdraw consent.

24. Where consent is required in relation to pupils, we seek consent from the parent/s of the pupil until the pupil has sufficient understanding to make their own decision. Typically, a child of 12 years of age will have reached a sufficient level of understanding but a decision will be made in each individual case about a child's capacity. In general, a child isn't considered to have sufficient capacity if it's clear that they are acting against their own best interests. Where possible we will keep the parent informed and take into account any objections from the parent. We will not normally go against the wishes of the parent unless the circumstances are such that after careful consideration we conclude that it is both lawful and in the best interests of the child.

Data integrity

25. The School undertakes to ensure data integrity by the following methods.

Data accuracy

26. Data held will be as accurate and up to date as is reasonably possible. Every reasonable step will be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay. If a data subject informs the School of a change of circumstances, their electronic record will be updated as soon as is practicable. Parents and staff can view their personal details (on Bromcom and Every HR respectively) and request or make changes directly.

27. Where a data subject challenges the accuracy of their data, the School will immediately mark the record as potentially inaccurate, or 'challenged'. In the case of any dispute, we shall try to resolve the issue informally, but if this proves impossible, disputes will be investigated using the data protection complaints procedure. Until resolved the 'challenged' marker will remain and all disclosures of the affected information will contain both versions of the information.

Data adequacy and relevance

28. 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, including via our privacy notices. 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.

29. Staff must only process personal data where it is necessary in order to do their jobs. When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the school's record retention schedule.

Data retention

30. Data held about individuals will not be kept for longer than necessary for the purposes registered. We have adopted a Records Retention Schedule, which sets out the time period for which different categories of personal data are kept. It is the duty of members of the Senior Leadership Team (SLT) to ensure that obsolete data are properly erased in the business areas for which they are responsible.

Data disposal

31. The School recognises that the secure disposal of redundant data is an integral element to compliance with legal requirements and an area of increased risk. All data held in any form of media (paper, tape, electronic) shall only be passed to a disposal partner with demonstrable competence in providing secure disposal services.

32. All data shall be destroyed or eradicated to agreed levels meeting recognised national standards, with confirmation at completion of the disposal process. Disposal of IT assets holding data shall be in compliance with ICO guidance:

33. The school uses an external contractor to dispose of sensitive data that is no longer required and there is a cross shredder for the purposes of shredding confidential information on-site.

34. For further information on disposal procedures, staff should refer to the Secure Disposal of IT Equipment and Information Policy.

The Crypt School Archive

35. The Crypt School Archive is maintained as a resource to help inspire and equip current staff and pupils to understand and appreciate issues of identity, belonging and shared heritage; to prompt memories of school life among many generations of old Cryptians; and to serve as a research resource for all interested in the history of The Crypt School and the community it serves. The archive contains limited information (photo, dates of attendance at the School, exam records, last provided confidential information sheet and the pupil's destination after school, if provided) about former pupils of the School, which is extracted from pupil records after the pupil reaches 25 years of age.

36. Unless the data subject has given their consent (with proof of identity), access to personal data in this archive by someone other than the data subject or archive administrators will only be allowed after assessment of the purpose of the request and the likely impact on the data subject's right of privacy. Access will usually not be possible until the data subject is, or can be presumed to be, deceased (assuming a lifespan of 100 years). Decisions on requests to access personal data in the archive will be taken by the Deputy Headmaster. This policy has been drawn up in line with The National Archives *Guide to Archiving Personal Data* (August 2018).

Data and computer security

37. Security of data shall be achieved through the implementation of proportionate physical and technical measures. The IT Manager is responsible for the effectiveness of the controls implemented and reporting of their performance. The security arrangements of any organisation with which data is shared shall also be considered and, where required, these organisations shall provide evidence of the competence of data security.

38. The Crypt School undertakes to ensure security of personal data by the following methods.

Physical security

39. Appropriate building security measures are in place, such as alarms, window bars, deadlocks and computer hardware cable locks. Only authorised persons are allowed in the computer room. Storage devices and printouts are locked away securely when not in use. Medical information that may require immediate access during the school day is kept in a locked cupboard in Reception. Visitors to the School are required to sign in and out, to wear identification badges whilst in the School and are, where appropriate, accompanied.

40. **At all times, in and out of school, staff are responsible for the school data that they use in their day-to-day work.** This includes, but is not restricted to examples such as printed data, data on memory sticks, electronic equipment etc. Sensitive or personal information and data should not be removed from the school site, however the school acknowledges that some staff may need to transport data between the school and their home in order to access it for workout of school hours or off-site.

41. The following guidelines are in place for staff in order to reduce the risk of personal data being compromised:
    - Paper copies of personal information should not normally be taken off the school site. If these are misplaced they are easily accessed. If there is no way to avoid taking a paper copy of data off the school site, the information should not be on view in public places, or left unattended under any circumstances.
    - Unwanted paper copies of data, sensitive information or pupil files should be shredded. This also applies to handwritten notes if the notes reference any other staff member or pupil by name.
    - Care must be taken to ensure that printouts of any personal or sensitive information are not left in printer trays or photocopiers.
    - If information is being viewed on a PC, staff must ensure that the window and documents are properly shut down before leaving the computer unattended. Sensitive information should not be viewed on public computers.
    - Laptops and USB sticks that staff use must be encrypted and password protected.

42. These guidelines are clearly communicated to all school staff, and any person who is found to be intentionally breaching this conduct will be disciplined in line with the seriousness of their misconduct.

Logical security

43. Security software is installed on all computers containing personal data. Only authorised users are allowed access to the computer files and where possible are protected by multi-factor authentication. Computer files are backed up (ie security copies are taken) regularly.

Procedural security

44. In order to be given authorised access to the computer, staff will have to confirm that they have read and accepted the School's Acceptable Use Policy and Data Protection Policy. All staff are trained in their Data Protection obligations and their knowledge updated as necessary. Computer printouts as well as source documents containing personal data are shredded before disposal.

Data breaches

45. A data breach occurs when a breach of security leads to the accidental or unlawful loss, destruction, alteration, disclosure of, or unauthorized access to, personal data. Data breaches can have serious effects on the individuals or institutions concerned and may result in criminal prosecution and fines for the School and the individuals involved.

46. The School will make all reasonable endeavours to ensure that there are no personal data breaches. All potential or confirmed data breach incidents should be reported and recorded in the School's data breach log. All incidents will be investigated, the potential impact assessed, and appropriate remedial action taken.

47. All staff and volunteers are expected to follow the School's procedures for reporting potential or known data breaches via the School Data Breach Reporting Form on the School's intranet staff page. The IT Manager supported by the Compliance Officer is responsible for the initial investigation and recording of data breaches, working in liaison with the Data Protection Officer when the breach needs to be notified to the Information Commissioner's Office (ICO) or the individual concerned.

<u>Data Protection Rights of the Individual</u>

Data access requests (subject access requests)

48. Any individual whose data is held by us has a legal right to request access to such data or information about what is held. A request for personal data ("subject access request" or SAR) may be submitted to the School verbally or in writing; we provide a Subject Data Access Request form on the School website (or from the School office, 01452 530291) to facilitate this process. Ordinarily no charge will be made to process the request but, where requests are manifestly unfounded or excessive, in particular because of their repetitive character, the School can either (a) refuse to act on the request or (b) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested. The School must make a "reasonable and proportionate search" for the requested information and must respond within one month of receipt of the request. We may extend the time limit by up to a further two months where necessary, if the request is complex or we receive a number of requests from the person; we

will notify the person within the original one-month period with reasons if this is the case.

Requests for information about children

49. An individual is only entitled to their own personal data, and not to information relating to other people. In responding to requests concerning children, the School will consider whether the child is competent to make a SAR (that is, are they mature enough to understand their rights); and the nature of the information requested. If a child is competent, they may authorize a parent, guardian or other representative to make a SAR on their behalf; the School will require evidence of this authorization before releasing any information. In all cases, the School will put the child's best interests first and protect their rights, welfare and privacy when taking any decision about whether to disclose a child's personal information.

Other data protection rights of the individual

50. 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, or object to the processing of it (in certain circumstances)
    - Prevent use of their personal data for direct marketing
    - Challenge processing which has been justified on the basis of public interest
    - Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
    - Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
    - Prevent processing that is likely to cause damage or distress
    - Be notified of a data breach in certain circumstances
    - Make a complaint to the ICO
    - Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)
    - Where personal data is no longer required for its original purpose, an individual can demand that the processing is stopped, and all their personal data is erased by the school including any data held by contracted processors.

Responsibilities

51. The Governing Body of the School has overall responsibility for ensuring that records are maintained, including security and access arrangements, in accordance with education, data protection and other relevant statutory provisions. The Governing Body receives regular reports on the implementation of data protection measures, including the findings of internal audits and other monitoring activities, and data on breaches and subject access requests.

52. The School has appointed Gloucestershire County Council as its Data Protection Officer

(DPO). The DPO is an independent role, reporting directly to the Governing Body. The School's DPO can be contacted on 01452 583619 or schoolsdpo@gloucestershire.gov.uk

53. The Compliance Officer is responsible for developing and implementing the programme to deliver data protection legislation requirements in the School. **The DPO works alongside the Compliance Officer to:**

a. Educate the whole school community in relation to data protection;
b. Serve as the point of contact between the school and Data Protection Supervisory Authorities and third parties;
c. Support the Compliance Officer to monitor performance, providing advice on the impact of data protection efforts;
d. Support the Compliance Officer in interfacing with data subjects to inform them about how their data is being used, their rights, and what measures the School has put in place to protect their personal information;
e. Support and inform policy and practice for risk and data breaches.

54. The Senior Leadership Team is responsible for:

a. fostering a culture of personal responsibility and commitment related to data protection in the School;
b. ensuring that data protection requirements are implemented in the business processes for which they are responsible; and
c. ensuring that staff are aware of the information security and data protection policies that affect them and that they attend or complete training as required.

55. The IT Manager is responsible for designing and delivering measures relating to the security of personal data in the School environment and the audit of data processing activities.

56. All staff, volunteers and people working on the School site are responsible for this policy's implementation. All the School's staff have a personal responsibility to:

a. handle personal data in accordance with the School's data protection and information security policies;
b. complete data protection and information security induction training and continue to attend or complete training as required;
c. notify new categories of personal data processing activities to the Compliance Officer;
d. report security incidents or weaknesses and potential or known data breaches immediately on becoming aware of them; and
e. understand that failure to comply with information security and data protection policies is treated seriously and deliberate breaches can lead to disciplinary action.

Training

57. All staff are required to complete data protection awareness training. Staff with particular responsibilities for handling personal data (for example, in relation to human resources,

admissions and the School's management information system) undertake more detailed training.

Planning and monitoring

58. Internal audits of personal data processing activities shall be undertaken on a regular basis to monitor compliance with this policy and data protection legislation. The findings of audits shall be used supportively to strengthen data protection and information practice across the School.

59. The School will carry out data protection impact assessments (DPIAs) when using new technologies and when processing is likely to result in a high risk to the rights and freedoms of individuals and in particular in every situation when a DPIA is required by the Information Commissioner's Office.

Enquiries and complaints

60. Information about the school's Data Protection Policy is available from the Clerk to the Governors (clerk@crypt.gloucs.sch.uk; tel. 01452 530291). General information about the GDPR can be obtained from the Information Commissioner's Office (Helpline 0303 123 1113, website www.ico.gov.uk).

61. Complaints about how a subject access request was handled, data security measures during a breach, or the collection, use or retention of your personal data, may be submitted via email to foi@crypt.gloucs.sch.uk. We ask that complaints are submitted using the headings on the data protection complaints form at Appendix 1 (also available on the school website under Policies and Forms); but complaints submitted via any route will be accepted.

62. Complaints will be handled by a senior member of staff at the School, who will work closely with our Data Protection Officer to investigate the concerns raised.

63. The complaint will be acknowledged and assigned to a member of the Senior Leadership Team within 30 days. If necessary, the complaint will be clarified. Should the complaint not be clarified within 21 days, then the school will consider the matter closed with no further action required.

64. The School will work closely with the Data Protection Officer to investigate the complaint, maintaining open communication with the complainant, if required, throughout the process. Following the investigation, the School will let the complainant know the outcome without unjustifiable or unreasonable delay.

65. If the complainant remains dissatisfied following the internal investigation, they will be provided with the Information Commissioner's Office contact details to enable them to submit a formal complaint.

Approved by Trustees Pupil Education & Outcomes Committee: November 2026
Review cycle: 2 years
Date of next review: June 2028

APPENDIX 1: DATA PROTECTION COMPLAINTS FORM

Please complete and return to the Compliance Officer (foi@crypt.gloucs.sch.uk) or the School Office (enquiries@crypt.gloucs.sch.uk)

Your name:
Address: **Postcode:** **Day time telephone number:** **Evening telephone number:** **Email address:**
Please give details of your complaint, including whether you have spoken to anybody at the school about it.

What actions do you feel might resolve the problem at this stage?
Are you attaching any paperwork? If so, please give details.
Signature: **Date:**
Official use
Date acknowledgement sent:
By who:
Complaint referred to:

Action taken:
Date: