The Crypt School Data Protection Policy

Lead Persons: Gordon Taylor, IT Manager; Nicola Donlon, Compliance Officer
SLT Member Responsible: Deputy Headmaster
Governing Body Committee: Pupil Welfare

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 EU General Data Protection Regulation (GDPR) and other data protection legislation. "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.

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.

Scope

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 **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 data protection principles

6. The 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
- adequate, relevant and limited to what is necessary
- accurate and, where necessary, up to date
- kept in a form that permits identification for no longer than is necessary
- processed in a way that ensures appropriate security

7. As a data controller, the School must also be able to demonstrate compliance with these principles ("accountability" principle).

Fair obtaining and processing

8. 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. Information about the use of personal data is also included on the appropriate collection form.

9. 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, local authorities or the Department for Education. This is set out in our privacy notices.

Consent to process personal data

10. 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.

11. 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. Ordinarily, a child of 12 years of age will have reached a sufficient level of understanding but children who have special educational needs which affect their ability to understand may not have sufficient understanding until later. 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

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

Data accuracy

13. 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 computer record will be updated as soon as is practicable. A printout of contact data records will be provided to pupils, parents and staff every twelve months so they can check their accuracy and make any amendments.

14. 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 referred to the Governing Body for their judgment. If the problem cannot be resolved at this stage, either side may seek independent arbitration. 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

15. Data held about people will be adequate, relevant and not excessive in relation to the purpose for which the data is being held. In order to ensure compliance with this principle, the School will check records regularly for missing, irrelevant or seemingly excessive information and may contact data subjects to verify certain items of data. The IT Manager and Compliance Officer will undertake regular random checks of records to ensure that they comply with our collection and retention guidelines.

16. 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 SLT to ensure that obsolete data are properly erased in the business areas for which they are responsible.

Data and computer security

17. 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 organization with which data is shared shall also be considered and, where required, these organisations shall provide evidence of the competence of data security.

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

Physical security

19. 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. Disks, tapes and printouts are locked away securely when not in use. Visitors to the School are required to sign in and out, to wear identification badges whilst in the School and are, where appropriate, accompanied.

Logical security

20. Security software is installed on all computers containing personal data. Only authorised users are allowed access to the computer files and password changes are regularly undertaken. Computer files are backed up (ie security copies are taken) regularly.

Procedural security

21. In order to be given authorised access to the computer, staff will have to sign an information security and data protection statement. All staff are trained in their Data Protection obligations and their knowledge updated as necessary. Computer printouts as well as source documents are shredded

before disposal.

Data breaches

22. 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.

23. 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. Individual members of staff may also be subject to claims for damages from persons who believe that they have been harmed as a result of inaccuracy, unauthorised use or disclosure of their data.

24. All staff and volunteers are expected to follow the School's procedures for reporting potential or known data breaches, which are published on the School's portal. The IT Manager 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.

Data access requests (subject access requests)

25. Any individual whose data is held by us has a legal right to request access to such data or information about what is held. We shall respond to such requests within one month and they should be made in writing on a Subject Data Access Request form (available from the School office, 01452 530291) and submitted to the IT Manager. Ordinarily no charge will be made to process the request but note that 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

26. Where a request for subject access is received from a pupil, the School's policy is that:
    • Requests from pupils will be processed as any subject access request as outlined below and the copy will be given directly to the pupil, unless it is clear that the pupil does not understand the nature of the request.
    • Requests from pupils who do not appear to understand the nature of the request will be referred to their parents or carers.

Responsibilities

27. 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.

28. 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, with responsibility to advise the School on its obligations under data protection legislation; monitor compliance; advise on data protection impact assessments; train staff; conduct internal audits; and be the first point of contact for supervisory authorities and for individuals whose data is processed.

29. The School's DPO can be contacted on 01452 583619 or schoolsdpo@gloucestershire.gov.uk

30. 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. Work with the School in maintaining comprehensive records of all data processing activities conducted by the School, including the purpose of all processing activities, which must be made public on request;
    e. 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;
    f. Support and inform policy and practice for risk and data breaches.

31. 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.

32. 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.

33. 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

34. 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

35. 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.

36. Certain staff with particular responsibilities for handling personal data shall undertake annual self-assessments to measure levels of assurance against a range of control measures.

37. 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.

Documentation

38. The School maintains an information register, which documents for higher risk processing activities:
    a. The purposes for which we use personal data;
    b. The different types of people whose personal data is processed;
    c. The categories of personal data processed (e.g. contact details, financial information, health data);
    d. The categories of recipients of personal data held by the School (whom we share personal data with);
    e. Our retention schedule for different categories of personal data.

39. The School also maintains a register of data breaches.

40. 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 the GDPR 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 GDPR.

Enquiries

41. 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).

Approved by Full Governors: [July 2018]
Date of next review: [July 2019]