CHATHAM & CLARENDON GRAMMAR SCHOOL

Secure Data Handling Policy

Ratified by Governors: November 2018

INTRODUCTION

1. The Chatham & Clarendon Grammar School (the School) acknowledges that to function properly we need to collect and use certain types of information about staff, students and other individuals who come into contact with the School.

2. We are also obliged to collect and use data to fulfil our obligations to the local authority (LA), DfE and other bodies.

3. 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.

4. The School aims to ensure that all personal data collected about staff, students, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.

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

6. This policy should be read in conjunction with the following School policies, all of which can be found on the Data Protection page of the school website
   - General Data Protection Regulations Policy
   - Retention of Records Policy
   - Freedom of Information Publication Scheme
   - Privacy Notices for:
     - Parents
     - Students
     - Staff and Volunteers

7. 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.

8. The School's DPO is Ms J Dawes, Clerk to the Governors, and is contactable at gdpr@ccgrammarschool.co.uk

9. It is the responsibility of all members of the School community to take care when handling, using or transferring personal data so that it cannot be accessed by anyone who does not:
    - Have permission to access that data
    - Need to have access to that data

10. Any loss of personal data can have serious effects for individuals and/or the School. It can bring the School into disrepute and may well result in disciplinary action and/or criminal prosecution for individuals. All transfer of data is subject to risk of loss or contamination.
11. Anyone who has access to personal data must know, understand and adhere to this policy, which brings together the legal requirements contained in current relevant data legislation and regulations. The loss of personal data by organisations and individuals over the last few years has made this a relevant and high profile issued for schools and all organisations. It is important that the School has a clear and well understood personal data policy because:

    - No school or individual would want to be the cause of any loss of personal data, particularly as the impact of data loss on individuals can be severe and cause extreme embarrassment, put individuals at risk and affect personal, professional or organisational reputation.
    - Schools are 'data rich' and the introduction of electronic storage and transmission of data has created additional potential for the loss of data.
    - The School will want to avoid the criticism and negative publicity that could be generated by any loss of personal data.
    - The School is subject to a wide range of legislation related to data protection and data use, with significant penalties for failure to observe the relevant legislation

12. Schools have always held personal data on the students in their care, and increasingly this data is held digitally and accessible not just in school but also from remote locations.

13. The School and individuals working in the School will have access to a wide range of personal information and data. The data may be held in digital format or on paper records. Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances. This can include:

    - Personal information about members of the School community – including students, members of staff, parents and carers e.g. names, addresses, contact details, legal guardianship, health records, disciplinary records
    - Curricular/academic data e.g. class lists, student progress records, reports, references
    - Professional records e.g. employment history, taxation and national insurance

records, appraisal records and references
- Information that might be disclosed by parents/carers or by other agencies working with families or staff members

Principles

14. As the role of Schools management information systems (SIMS) continues to develop, staff in schools have increasing access to a wide range of sensitive information. There are generally two types of sensitive information including (but not limited to):
- Personal data concerning the staff and students
- Commercially sensitive financial data

15. It is important to ensure that both types of information are managed in a secure way at all times. Personal data is the most likely form of sensitive data that a school will hold. Personal data is defined by the GDPR as 'Any information relating to an identified, or identifiable, individual'. The GDPR is based on data protection principles with which the School must comply.

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

17. The GDPR states that some types of personal information demand an even higher level of protection and are referred to as special categories of personal data. This includes information relating to:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetics
- Biometrics (such as fingerprint, retina and iris patterns), where used for identification purposes NB: full fingerprint information is not collected
- Health – physical or mental
- Sex life or sexual orientation

18. The three questions below can be used to quickly assess whether information needs to treated securely:

- Would disclosure/loss place anyone at risk?
- Would disclosure/loss cause embarrassment to an individual or the School?
- Would disclosure/loss have legal or financial implications?

19. If the answer to any of the above is 'yes', then it will contain personal or commercially sensitive information and needs a level of protection.

Purpose

20. The purpose of this policy is to advise all members of staff what is required by the School to ensure that it complies with the GDPR at all times and to advise all members of staff how to proceed when handling data which needs to be handled securely.

Procedures and practice

21. The following practices will be applied within the School:

- All personal data will be fairly obtained in accordance with the privacy notices and lawfully processed
- The amount of data held by the school will be reduced to a minimum
- Data held by the school must be routinely assessed to consider whether it still needs to be kept or not
- Personal data held by the school will be securely stored and sent by secure means
- Every effort will be made to ensure that the data held is accurate, up-to-date and that inaccuracies are corrected without unnecessary delay.

Auditing

22. The School must be aware of all the sensitive data it holds, be it electronic or paper. Therefore:

- A data asset register will be kept within school detailing the types of sensitive data held, where and by whom, and will be added to as and when new data is generated. This register will be checked by the relevant information asset owner each year and revisions made accordingly.
- The length of time that individual sensitive documents need to be kept will be assessed in accordance to the retention of records policy.

Risk assessment

23. The School will regularly carry out a risk assessment to establish what security measures are already in place and whether or not they are the most appropriate and cost effective available. The School's DPO is responsible for the completion of the risk assessment.

24. The School's risk assessment will generally involve answering the following questions:

- How sensitive is the data?
- What is the likelihood of it falling into the wrong hands?
- What would be the impact of the above?
- Does anything further need to be done to reduce the likelihood?

25. When these questions have been answered, the DPO will be able to recognise the risks that are present, judge the level of those risks and prioritise them. Once the risk assessment has been completed, the School will decide how to reduce any risks or whether they are at an acceptable level.

26. Appendix 1 provides staff with a help sheet for assessing the risk of sharing information.

27. Risk assessment will be an on-going process and the School will carry out assessments at regular intervals because risks change over time.

Securing and handling data held by the school

28. The School will encrypt any data that is determined to be personal or commercially sensitive in nature. This includes data held on fixed station computers, laptops, portable devices and memory sticks.

29. All staff will be trained to understand the need to handle data securely and the responsibilities incumbent on them. This will be the responsibility of the DPO.

30. The School has a clear policy and a procedure for the use of cloud-based storage systems, and is aware that data held in remote cloud storage is still required to be protected in line with the GDPR. The School will ensure that it is satisfied with the controls put in place by service providers to protect the data.

31. Biometric data complies with the same data protection principles outlined above and also with the Protection of Freedoms Act 2012. We will ensure that each parent of a student at the School is notified if we use their child's biometric data as a part of our automated biometric information system. Written consent of the parents is obtained before the data is taken from all pupils under 18 years of age. We will not process this data if the child under 18 (if deemed competent to understand the issue) refuses or if no parents have consented in writing. The School provides alternative means of accessing services for those pupils who will not be using an automatic biometric recognition service.

32. Staff should not copy or remove sensitive data from the School or authorised premises unless the data and/or media is:

- Encrypted
- Transported securely
- Stored in a secure location

33. Sensitive data should not be transmitted in unsecured emails.

34. Data transfer should be through secure websites. If this is not available, then the file must be minimally password protected or preferably encrypted before sending via email. The password must be sent by other means, and on no account included in the same email. A record of the email should be kept to identify when, and to whom, the email was sent.

35. Data (student records, SEND data, contact details, assessment information) must be automatically backed up, encrypted and stored in a secure place, e.g. safe/fire safe/remote backup facility.

36. All staff computers, including laptops, must be used in accordance with the policies for ICT and use of the internet and intranet by staff.

37. When laptops are passed on or re-issued, data will be securely wiped from any hard drive before the next person uses it (not simply deleted). This will be done by the school's Network Team support staff.

38. The School's wireless network (Wi-Fi) will be secure at all times.

39. The School will identify which members of staff are responsible for data protection (also known as information asset owners).

40. The School will ensure that staff who are responsible for sets of information, such as SEND, medical, vulnerable learners, management data etc. know what data is held, who has access to it, how it is retained and disposed of.

41. Where a member of staff has access to data remotely, the remote access off the School site to any personal data should be over an encrypted connection (e.g. VPN) protected by a username/ID and password. This School data must not be stored on a personal (home) computer.

42. Members of staff who are given full, unrestricted access to the school's management information system must access the systems over an encrypted connection.

43. The School will keep necessary student and staff information in accordance with the Retention of Records Management Policy.

44. The School will securely delete commercially sensitive or personal data when it is no longer required according to the Retention of Records Management Policy.

APPENDIX 1

Staff help sheet for assessing risk of sharing information

In deciding the most appropriate way to share information and the level of security required, always take into consideration the nature of the information and the urgency of the situation, that is, take a risk-based approach to determining appropriate measures. The simplified process described below will help members of staff and the school itself choose the appropriate level of security needed when sharing potentially sensitive information. The Data Protection Officer is responsible for ensuring that staff are trained to use this process.

Step 1

Imagine a potential security breach (e.g. a confidential letter is left in a public area, a memory stick is lost or someone reads information on a computer screen while waiting to meet a member of staff), and consider:

- Will it affect or identify any member of the school or community?
- Will someone suffer a financial loss?
- Will it cause any kind of criminal case to fail?
- Is there a risk of discomfort/slur upon professional character of someone?
- Is anyone's personal safety at risk?
- Will it embarrass anyone?

If the answer to all the above questions is 'no', the document does not contain sensitive information.

If the answer is 'yes' to any of the questions above then the document will include some sensitive information and therefore requires a level of protection.

Step 2

Imagine the same potential security breach as above, and consider:

- Will it affect many members of the school or local community and need extra resources locally to manage it?
- Will an individual or someone who does business with the school lose/be out of pocket by £1,000 to £10,000?
- Will a serious criminal case or prosecution fail?
- Is someone's personal safety at a moderate risk?
- Will someone lose his or her professional reputation?
- Will a company or organisation that works with the school lose £100,000 to £1,000,000?

If the answer to any of the above questions is 'yes' then the document contains sensitive information and additional security should be considered such as password protecting the document before you email it to a colleague outside of the school. However, if you think that the potential impact exceeds that stated in the question (e.g. someone's personal safety is at high risk) think very carefully before you release this information at all.

Step 3

All documents that do not fit into steps 1 or 2 might require a higher level of protection/security if released at all. Err on the side of caution and seek guidance from the relevant line manager/senior member of staff.