Griffin Schools Trust

Data Protection, GDPR and Data Security Policy

Date: October 2019
Next review: October 2021
Approved by: Board of Trustees

Contents

1. Introduction

1.1 This policy is intended to clarify the obligations of the Griffin Schools Trust (the "Trust") under the Data Protection Act 2018 ("the Act") and the General Data Protection Regulation (GDPR). Everyone has rights with regard to how their personal information is handled. During the course of our activities we will collect, store and process personal information about a number of different groups of people and we recognise the need to treat it in an appropriate and lawful manner.

1.2 The types of information that we may be required to handle include details of current, past and prospective employees, pupils, parents, trustees, governors, volunteers, suppliers and other individuals that we communicate with. The information, which may be held on paper, on a computer or other media, is subject to certain legal safeguards specified in the GDPR and the Act and other regulations, which impose restrictions on how we may use that information.

1.3 The Trust has notified the Information Commissioner that it processes personal information, and is on the register of data controllers. The Trust will amend the entry if it becomes inaccurate, incomplete or requires renewal.

2. Scope

2.1 This policy shall apply in its entirety to all employees including headquarters staff, agency workers, contractors, governors and volunteers who shall be referred to in this policy as "staff".

2.2 In this policy "school" means any of the schools within the Trust.

2.3 This policy does not form part of any employee's contract of employment and it may be amended at any time. Any breach of this policy will be taken seriously and may result in disciplinary action. Breach of the GDPR or the Act may expose the Trust to enforcement action by the Information Commissioner or fines. Furthermore, certain breaches can give rise to personal criminal liability for the Trust's employees.

3. Responsibilities

3.1 All staff must read this policy carefully and make sure that they understand it.

4. Definition of Terms

4.1 Data is information which is stored electronically on a computer or in certain paper-based filing systems.

4.2 Data subjects for the purpose of this policy include all living individuals about whom we hold personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal data.

4.3 Personal data means data relating to a living individual who can be identified from that data on its own or when taken together with other information. Personal data can be

factual (such as a name, address or date of birth) or it can be an opinion (such as a school report) and can include telephone numbers, photographs and CCTV images.

4.4 Data controllers are the people who, or organisations which, determine the purposes for which, and the manner in which, any personal data is processed. They have a responsibility to establish practices and policies in line with the Act. The Trust and Schools are the data controller of all personal data used in the Trust.

4.5 Data users include employees whose work involves using personal data. Data users have a duty to protect the information they handle by following our data protection and security policies at all times.

4.6 Data processors include any person who processes personal data on behalf of a data controller. Employees of data controllers are excluded from this definition, but it could include suppliers which handle personal data on our behalf.

4.7 Processing is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

4.8 Special categories of personal data includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, genetic or biometric data, physical or mental health or condition or sexual life and sexual orientation. Special categories of personal data can only be processed under strict conditions. Data about criminal convictions and offences are not included under the definition of special categories of personal data but similar safeguards apply and therefore for the purposes of this policy are treated in the same way.

5. Data Protection Principles

5.1 Anyone processing personal data must comply with the six Data Protection Principles. These provide that personal data must:

- be processed fairly, lawfully and transparently;
- be collected and processed only for specified, explicit and legitimate purposes;
- be adequate, relevant and limited to what is necessary for the purposes for which it is processed;
- be accurate and kept up to date;
- not be kept longer than necessary for the purposes for which it is processed;
- be processed securely.

6. Fair and Lawful Processing

6.1 The GDPR is intended not 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. The data subject must be provided with certain information, including who the data controller is (in this case the Trust), the purpose for which the data is to be processed by us and the identities of anyone to whom the data may be disclosed or transferred.

6.2 For personal data to be processed lawfully, certain conditions have to be met. These may include, among other things, requirements that the data subject has consented to the processing, or that the processing is necessary for the legitimate interest of the data controller or the party to whom the data is disclosed. When special categories of personal data are being processed, more than one condition must be met. In some cases the data subject's explicit consent to the processing of such data will be required.

6.3 Fair and lawful processing of data includes having legitimate grounds for collecting and using the personal data, not using the data in ways that have unjustified adverse effects on the individuals concerned, being transparent about how you intend to use the data and handling personal data only in ways they would reasonably expect.

7. Accurate Data

7.1 Personal data must be accurate and kept up to date. Information which is incorrect or misleading is not accurate and steps should therefore be taken to check the accuracy of any personal data at the point of collection and at least annually afterwards. Inaccurate or out-of-date data should be destroyed. If a data subject informs the Trust of a change of circumstances their computer record will be updated as soon as is practicable.

7.2 Where a data subject challenges the accuracy of their data, the Trust 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 relevant Local Governing Body for their judgement. 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.

7.3 Notwithstanding paragraph 7.2, a data subject continues to have rights under the Act and may refer a complaint to the Information Commissioner's Office regardless of whether the procedure set out has been followed.

8. Timely Processing

8.1 Personal data should not be kept longer than is necessary for the purpose for which it is held. This means that data should be destroyed or erased from our systems when it is no longer required, in accordance with our data retention schedules

9. Processing in Line with Data Subject's Rights

9.1 Data must be processed in line with data subjects' rights. Data subjects have a right to:

- request access to any data held about them by a data controller;
- object to processing based on legitimate interests, the performance of a task in the public interest, for direct marketing purposes or the purposes of scientific or historical research and statistics;
- ask to have inaccurate data amended, completed (if it is incomplete) or erased;
- ask for their personal data to be moved, copied or transferred from one IT environment to another in a safe and secure way;
- request the restriction or suppression of their personal data.

Data subjects also have certain rights in relation to automated decision making, including profiling. We do not currently use automated decision making in any of our processing activities.

Some of the rights described above are not absolute and will be subject to, amongst other things, the legal basis for processing the personal data.

A data subject can exercise these rights by contacting the Data Protection Compliance Manager at their school.

10. Data Security

10.1 The Trust has taken steps to ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

10.2 The GDPR and the Act requires us to put in place procedures to maintain the security of all personal data from the point of collection to the point of destruction. Personal data may only be transferred to a third-party data processor if they agree to comply with those procedures and policies, or if they put in place adequate measures themselves.

10.3 Maintaining data security means guaranteeing the confidentiality, integrity and availability of the personal data, defined as follows:

- confidentiality means that only people who are authorised to use the data can access it;
- integrity means that personal data should be accurate and suitable for the purpose for which it is processed;
- Availability means that authorised users should be able to access the data if s/he need it for authorised purposes. Personal data should therefore be stored on our central computer system instead of individual PCs.

10.4 Security procedures include:

- Physical Security: Appropriate building security measures are in place and only authorised persons are allowed in the computer rooms. Disks, tapes, hard drives, memory sticks 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;
- Computer Security: Only authorised users are allowed access to computer files and password changes are regularly undertaken. Computer files are backed up regularly. Data users should ensure that individual monitors do not show confidential information to passers-by and that s/he logs off from their PC when it is left unattended;
- Procedural Security: In order to be given authorised access to the computer systems, staff will have to undergo checks and will sign a confidentiality agreement. 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. CD-ROMs and portable drives are physically destroyed when they are no longer required.

11. Dealing with Subject Access Requests

11.1 The GDPR extends to all data subjects a right of access to their own personal data. A request from a data subject for information that we hold may be received verbally or in writing. A fee cannot be charged for provision of this information except in certain limited circumstances. Any member of staff who receives a written request should forward it to their Head immediately as there are statutory time limits for responding (currently one month).

11.2 In order to ensure that people receive only information about themselves it is essential that a formal system of requests is in place. Where a request for subject access is received from a pupil, the Trust's policy is that:

- Requests from pupils who are considered mature enough to understand their rights will be processed as any subject access request as outlined below and the copy will be given directly to the pupil. The Information Commissioner's guidance is that it may be reasonable to adopt a presumption that by the age of 12 a child has sufficient maturity to understand their rights and to make an access request themselves if s/he wishes. In every case it will be for the school to assess on behalf of the Trust whether the child is capable of understanding their rights under the Act and the implications of their actions, and so decide whether the parent needs to make the request on the child's behalf;
- Requests from parents in respect of their own child will be processed as requests made on behalf of the data subject (the child) and the copy will be sent in a sealed envelope to the requesting parent unless the school considers the child to be mature enough to understand their rights, in which case the school shall ask the child for their consent to disclosure of the personal data (subject to any enactment which permits the School to disclose the personal data to a parent without the child's consent). If consent is not given to disclose, the school shall not disclose the personal data if to do so would breach any of the data protection principles.

11.3 Following receipt of a subject access request, and provided that there is sufficient information to process the request, an entry will be made in the school's Subject Access log book, showing the date of receipt, the data subject's name, the name and address of requester (if different), the type of data required (e.g. Student Record, Personnel Record), and the planned date for supplying the information. Should more information be required to establish either the identity of the data subject (or agent) or the type of data requested, the date of entry in the log will be date on which sufficient information has been provided.

12. Providing Information over the Telephone

12.1 Any member of staff dealing with telephone enquiries should be careful about disclosing any personal information held by the Trust. In particular s/he should:

- check the caller's identity;
- suggest that the caller put their request in writing;
- refer the request and the caller's identity details to the Data Protection Compliance Manager or the Head/Head of School for assistance.

13. Authorised Disclosures

13.1 The Trust will only disclose data about individuals where it has identified a legal basis for doing so. The legal basis for processing personal data is set out in the relevant privacy notices provided to staff and pupils/parents.

13.2 Only authorised and trained staff are allowed to make external disclosures of personal data. Data used within the schools by administrative staff, teachers and welfare officers will only be made available where the person requesting the information is a professional legitimately working within the Trust who needs to know the information in order to do their work.

14. CCTV

14.1 The Trust uses CCTV in locations around its sites. This is to:

- safeguard pupils and staff
- protect the school buildings and their assets;
- increase personal safety and reduce the fear of crime;
- support the Police in a bid to deter and detect crime;
- assist in identifying, apprehending and prosecuting offenders;
- protect members of the public and private property;
- assist in managing the schools.

15. Enquiries

15.1 General information about the Act can be obtained from the Information Commissioner's Office, www.ico.gov.uk.

Useful References
The Data Protection Act 2018
The General Data Protection Regulation

16. Complaints

16.1 If you consider that the policy has not been followed in respect of personal data about yourself or others you should raise the matter with the relevant Data Protection Compliance Manager at your school or at the Griffin School Trust's Headquarters.

17. Review

17.1 The Trust will review this policy at least every two years and assess its implementation and effectiveness.

Appendix 1: Do's and Don'ts

Laptops and Workstations

Do

- Shut down your laptop or workstation using the 'Shut Down' or 'Turn Off' option;
- Try to prevent people from watching you enter passwords or view sensitive information;
- Turn off and store your laptop securely, even when travelling;
- Use a physical laptop lock if available to prevent theft;
- Lock your desktop when leaving your laptop or workstation unattended;
- Make sure your laptop, if it is likely to hold personal or sensitive data, is protected with encryption software;
- Secure your workstation when away from your work area through the use of a password protected screen saver, even if the plan is to return shortly;
- Use good password practices e.g. never keep your ID and password details with your laptop.

Don't

- Leave your laptop unattended unless there is adequate security in place;
- Use public wireless hotspots, they are not secure;
- Leave your laptop in your car. If unavoidable, lock it out of sight in the boot;
- Let unauthorised people use your laptop;
- Use 'hibernate' or 'standby' when away from your laptop.

Sending and Sharing Information

Do

- Be aware of who you are allowed to share information with;
- Encrypt all removable media that is removed from your school or sent by post or courier;
- Ensure that all USB memory drives are purchased with an encryption chip installed.

Don't

- Send sensitive information on removable media without encryption;
- Send sensitive information by email unless there is no alternative;
- Place protective labels on outside envelopes. Use an inner envelope if necessary so that people cannot see from the outside that the envelope contains sensitive information.

Paper Documents

Do

- Secure documents containing personal or sensitive personal data when not in use;
- Secure any documents or notes containing personal information that would cause damage or distress if it were lost or stolen.

Don't

- Leave documents containing personal information unattended on your workstation or at a photocopier;
- Disclose documents containing personal information to people who do not need to see them.
-

Appendix 2: Access to Personal Data Request Form

You should complete this form if you want us to provide you with a copy of your personal data, which we hold about you or your educational record.

We will endeavour to respond promptly to your request for personal data and in any event within one month of receipt of this completed form and satisfactory proof of identity where we request this.

We will endeavour to respond promptly to your request for your Educational Record and in any event usually within 15 school days of receipt of this completed form, satisfactory proof of identity and the required fee, if applicable.

Please tick the options that apply:

I am making this application for personal data about me (the Data Subject)	☐
I am requesting to see my Educational Record	☐
I am requesting a copy of my Educational Record	☐
I would like my agent to deal with my application on my behalf (I attach a signed authorisation of agent for subject access form)	☐

Please provide details for the person you are requesting information about:

Title:	Forename:	Surname:	
Date of Birth:		Telephone Number:	
Address:			Postcode:

Please provide a description of the sort of personal data, which you are seeking together with any dates from which we should search. We reserve the right, in accordance with the GDPR, to refuse to comply with a subject access request if it is manifestly unfounded or excessive, taking into account whether the request is repetitive in nature. Alternatively, we may charge a fee before we comply with the request. In either case we will inform you of the decision and the reasons for it.

State how you would like the reply to this request to be dealt with:

Sent to your home address (as stated)	☐
Collected from the school (you may be required to bring evidence to confirm your identity)	☐
Sent to your authorised agent (if appointed)	☐

Note: If the information you request reveals details directly or indirectly about another person, we will have to seek the consent of that person before we can let you see that information. In certain circumstances we may not be able to disclose the information to you, in which case you will be informed promptly and given full reasons for that decision.

I confirm that I have read and understand the terms of this subject access form.

Signature:		Dated:	
Name (use block capitals):			

Please return this form to your School Office or Griffin School Trust Headquarters, The Talent Factory, 4 – 14 Barmeston Road, London, SE6 3BH.

Appendix 3: Access to Educational Records Form

You will need to complete this form if you wish to access your child's Educational Record.

I am applying for a copy of the Educational Record of the Data Subject I confirm I *am the parent/*have parental responsibility of the data subject (*please delete as appropriate).	☐

Please provide details for the person you are requesting information about:

Title:	Forename:	Surname:	
Date of Birth:		Telephone Number:	
Address:			Postcode:

Enquirer Details (if you are not the data subject). Please provide your own details here:

Title:	Forename:	Surname:	
Date of Birth:		Telephone Number:	
Address:			Postcode:

I declare I *am the parent/*have parental responsibility for the above child and accept you may need to make further enquiries to validate this (*delete as appropriate). I have provided suitable proof of identity with this application.

Signature:	
Name (use block capitals):	
Date:	

Appendix 4: Authorisation of Agent for Subject Access

This application for Subject Access is made on behalf of:

Title:	Forename:	Surname:	
Date of Birth:		Telephone Number:	
Address:			Postcode:

I am the above-named person and authorise Griffin Schools Trust to give the information requested in this application to my agent whose name and address are given below.

Signature of person giving authority:	
Name (use block capitals):	
Date:	

AGENT:

Title:	Forename:	Surname:	
Date of Birth:		Telephone Number:	
Address:			Postcode:

What is your relationship with the data subject?	

I declare that I make this application on behalf of and solely in the interest of the named Data Subject. To ensure confidentiality I accept that you may need to make further enquiries to validate this authorisation. I have provided suitable proof of identity with this application.

Signature of agent:	
Name (use block capitals):	
Date:	

Appendix 5: Subject Access Request

Please complete the following and return to your School Office or Griffin School Trust Headquarters.

I am making enquires which are concerned with (tick the appropriate option)**:**

• The prevention and detection of crime	☐
• The apprehension or prosecution of offenders	☐

Nature of enquiry:

……

……

……

The information sought is needed to:

……

……

……

This enquiry is confidential and should not be communicated to the data subject

Name:			Tel No:	
Authority:			Position:	
Address:				
Signed:			Date:	
	(Block capitals)			
Countersigned:			Position:	
Name:			Date:	
	(Block capitals)			

Appendix 6: Consent to use Images of Children

Name of Child:	
Name of parent or guardian:	

From time to time we may take photographs of children at the school to use in our school prospectus, school or Trust website or other printed publications we produce. To comply with the GDPR and the Data Protection Act 2018, we need your permission before we can take any images of your child. Please answer the questions below by ticking the relevant box, sign the form and return to your child's Head of Year.

Please tick:

	YES	NO
May we use your child's photograph in the school prospectus and other printed publications that we produce for promotional purposes?	☐	☐
May we use your child's image on the Trust and/or academy website?	☐	☐

Please note that websites can be viewed throughout the world, not just in the United Kingdom where UK law applies. Please also note the conditions for using these images at the bottom of this form.

I have read and understood the conditions of use:

Signature of parent or guardian (for children under 12):		
Signature of data subject (for children over 12):		
Name (block capitals):		Date:

CONDITIONS OF USE

- This form is valid for five years from the date of signing. Your consent will automatically expire after this time, however you may withdraw your consent at any time;
- We will not include personal e-mail or postal addresses, or telephone or fax numbers on our website;
- We will not include details or full names (which means first name and surname) of any child or adult in an image on our website without good reason. For example, we may include the full name of a competition prize winner if we have their consent;
- If we use images of individual children, we will not use the name of that child in the accompanying text or photo caption without good reason. And if a child is named in the text, we will not use the image of that child to accompany the article without good reason (as in the example given above);
- We may use group or class photographs with very general labels, such as "a science lesson" or "art class";
- We will only use images of children who are suitably dressed, to reduce the risk of such images being used inappropriately;

Appendix 7: Data Protection Confidentiality Agreement

- Griffin Schools Trust has provided the information in confidence to you for the purpose of ..... and it must only be used for the stated purpose. The information remains the property of Griffin Schools Trust and must be returned or destroyed on completion;

- The information supplied constitutes personal data and must be processed in accordance with the principles of the GDPR and the Data Protection Act 2018;

- Appropriate measures must be taken to prevent the unlawful or unauthorised processing of the personal information supplied;

- On agreed completion, all copies of information should be returned or destroyed (as confidential waste) and deleted from your systems.

I agree to the terms of this Confidentiality Agreement

..... (Signature)

..... (Name)

..... (Date)