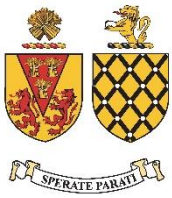
Watford Grammar School for Girls



Information Security Policy

Committee Responsible	Resources
Category	Statutory
Approved by Resources Committee	23.01.21
Approved by FGG (if statutory)	08.03.21
Review Cycle	3 Years
Next Review Date:	January 2024
Template:	unknown

Introduction

Watford Grammar School for Girls takes its responsibility to securely safeguard the information and data in its care, in particular personal data, very seriously. This document sets out our policy with regard to Information Security, and how we discharge our legal and moral responsibilities to safeguard it.

Watford Grammar School for Girls is an Academy Trust school, company number 07348254, registered office at Lady's Close, Watford, WD18 0AE, registered as a company in England and Wales, and an exempt charity. We are well known for our rich academic curriculum, our strong and supportive pastoral care, and the wide range of extended activities that, taken as a whole, educate, encourage and empower our girls. The school motto is *Sperate Parati* - or 'Go forward with preparation' - which encapsulates our aim for every member of the school community.

We are proud of the strong academic traditions and the importance of service to others that have shaped the ethos of our school since its foundation by Elizabeth Fuller in 1704. We value hard work and nurture scholarship, always encouraging our girls to achieve excellence in all fields of study. The girls have the opportunity to excel at music, drama and sport, as well as to play an active role in the wider community by taking part in many charitable activities. Thus they learn to be their best selves: hard working, compassionate and high achieving in all areas of life.

We are a diverse and thriving community, founded on consideration, toleration and trust. Each girl is given opportunities to develop confidence and resilience both in and outside the classroom, and to develop a sense of personal responsibility that is best summarised in the maxim 'I can do it, and I will do it' - words which every member of the school learns and takes to heart.

As part of ensuring the effective running of our school it is essential that we hold and use data and information about parents/carers, pupils, staff, governors, and others with whom we have relationships. It is important to us that we do this professionally and in line with our statutory, moral and contractual obligations, and that we safeguard that data and information securely, and this policy is part of how we explain how we do this. Legally the school is a Data Controller under the Data Protection Act 2018 / the General Data Protection Regulation, and the responsible officer at the school is Zia Rehman who is Data Protection Officer. The Data Protection Officer is also the responsible person at the school for Information Security.

This policy applies to related organisations the Women of Vision Trust (charity no. 1069040) as well as to the school.

1. Principles and Legislation

Our school aims to ensure that all data collected about staff, pupils, parents and visitors is collected, stored and processed in accordance with the General Data Protection Regulation / the Data Protection Act 2018. The school takes its responsibility to ensure the security of all information and data it processes very seriously, and this policy, produced in line with guidance issued by the Information Commissioner's Office, sets out how it does this.

This policy applies to all information and data, regardless of whether it is in paper or electronic format.

2. The Data Controller, Data Protection Officer and Information Security responsibility

Our school processes personal information relating to pupils, staff, parents, governors and others, and, therefore, is a Data Controller. Our school delegates the responsibility of data controller to the Deputy Head.

The school is registered as a Data Controller with the Information Commissioner's Office and renews this registration annually. You can check the register entry here.

The governing board has overall responsibility for ensuring that the school complies with its obligations under the General Data Protection Regulation / the Data Protection Act 2018, and for ensuring that this Information Security Policy is followed.

Day-to-day responsibilities rest with the headteacher, or the Deputy Head in the headteacher's absence. The headteacher will ensure that all staff are aware of their Information Security obligations.

In compliance with the GDPR / Data Protection Act, the School has an appointed Data Protection Officer who is responsible for dealing with any queries related to the storing or processing of personal data, and checking to ensure that the School is adhering to this policy and to its wider legal obligations. The Data Protection Officer is Zia Rehman.

Staff are responsible for ensuring that they handle any information and data in accordance with this policy. Staff are responsible for identifying and raising any new security risks associated with information they are working on whether electronic or paper-based, so that the school can take ensure that steps are taken to ensure appropriate security measures are in place.

The school acknowledges that from time to time contractors or agency staff may handle the school's information and data as part of discharging their duties to the school, and their supervisory member of staff or other designated staff contact is responsible for ensuring that they are aware of their Information Security responsibilities, that suitable contractual arrangements are in place to ensure these responsibilities are discharged and that the contractors or agency staff carry them out.

3. IT Systems: General Information Security

The school's IT systems are configured and managed so as to create and maintain the highest standards of Information Security, and in particular:

- The configuration of the school's IT network by its IT provider is such as to maximise Information Security
- The school's IT network is accessed via user accounts which are password protected. This includes laptops and other portable devices. Passwords must be at least 8 characters long and contain letters and numbers. Users are reminded to change their passwords at regular intervals. Users are only allowed to access those parts of the network essential for their work, minimising any security risks.
- The school's IT network uses a Firewall which is kept up to date, and Anti-Malware and Anti-Virus software which is also kept up to date

- The operating system(s) and software used by the school are kept up to date and in particular the most up to date patches and software updates are installed when practicable
- The school's IT network is regularly and securely backed up so as to be able to restore critical data in the event of any loss
- The school's IT provider monitors IT network use proactively and any suspicious patterns of activity which could pose a threat to Information Security can be identified and investigated
- From time to time users may need to access the school's IT network remotely. If staff need to work with information and data outside of the school building, they can do so by using the CC4 secure remote log-in to access the network drive. Staff who are authorised to do this are trained in the correct way of doing so.

4. Secure site, home and mobile working and portable data devices

The School maintains a secure site with any visitors escorted at all times and entry strictly controlled.

Within the site, information and data is subject to further physical safeguards: for example, filing cabinets and drawers containing particularly sensitive information on paper are kept locked with access restricted to staff who need it, and access to IT hardware is carefully managed with hardware securely stored when not in use.

The school understands that it is sometimes necessary to work at home or on the road with school paperwork, IT hardware or other equipment which contains information and data. Staff doing this will follow the appropriate home or mobile working policy/ the staff code of conduct when doing so. This includes a reminder to keep information and data, whether in electronic or paper form, secure at all times. Refresher training ensures that our longer-serving staff are regularly reminded of these requirements.

Removable media / portable data devices are occasionally used to transport data and information and the school understands that these can be at greater risk of loss or damage than when data is kept on the school's network. The school trains staff only to use such devices when there is no realistic alternative, to keep devices physically safe at all times, and to delete data from these devices when no longer needed.

The school recognises that there may be occasions when it is appropriate for a staff member to save personal data to their own device. Staff are provided with detailed guidance about how to keep personal data secure when using their own devices and are responsible for following this guidance.

5. Providers of outsourced IT or other services: general

The school will ensure that when any information or data is processed by or stored by an outsourced provider it is subject to at least as strict a set of Information Security procedures as it would be if stored on the school's own IT network. This will be ensured through the contract or arrangement between the school and the provider.

In addition, the school will ensure that information and data shall not be transferred to a country or territory outside the European Economic Area unless the country or territory also ensures an equivalent or adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data, in line with its obligations under the General Data Protection Regulation.

6. Paper records: general

Staff are required to take great care when handling paper-based records to ensure that the personal data in these records is not shared inadvertently. Papers containing confidential personal information should not be left on office and classroom desks, or on staffroom tables, or in any other place where they may be viewed other than by an authorised person.

7. Biometric data

As the School has a cashless catering system, we act as data controller for biometric data about pupils in this regard. Biometric data is classed as Sensitive Personal Data for the purposes of this Policy, and the School processes the data accordingly, see part 3 above.

The school operates this system for good reason: it avoids any difficulties with loss or theft or misplacement of lunch money, avoids distinction between pupils who do or do not receive free school meals, and facilitates an orderly and speedy provision of lunch as part of the school day. The School will make a considered assessment of any other use of biometric data systems if it considers introducing them, and the system will always require an opt-in for pupils to take part. The opt in clearly states what is being done, why, and how biometric data is protected.

The school's current biometric system providers, CRB Cunninghams, are the data processors for this data and hold it on their systems. CRB Cunninghams are accredited to ISO 27001 standard for Information Security.

A copy of the statement on the safeguarding of data provided by CRB Cunninghams is available on request from the Data Protection Officer, Zia Rehman.

8. Disposal of records

Information and records, electronic or paper, that are longer needed, or which have become inaccurate or out of date, and which are not required for the historical record, are disposed of securely.

For example, we shred or incinerate paper-based records, and override electronic files. We may also use an outside company to safely dispose of electronic or paper-based records.

9. Training

Our staff and governors are provided with Information Security training as part of their induction process.

Information Security will also form part of continuing professional development, where changes to legislation or the school's processes make it necessary. The headteacher is responsible for ensuring that staff are trained, aware of their Information Security responsibilities, and carry them out.

10. Incident Management and Reporting

The school works hard to avoid any Information Security breaches. However, it is ready, should any breach occur, to discharge its responsibilities under the General Data Protection Regulation / the Data Protection Act 2018 to notify the Information Commissioner's Office.

In addition, should any breach occur, the school would investigate this under the leadership of the Head Teacher, the Data Protection Officer and/or the Data Controller, make an internal report to the school's Senior Leadership Team, document the investigation and log its outcome, and address any issues which are identified as having contributed to the breach to avoid any repetition.

11. The General Data Protection Regulation

This policy has been updated in line with the new General Data Protection Regulation / the Data Protection Act 2018.

12. Monitoring arrangements

The Assistant Head, Curriculum and Data, is responsible for monitoring and reviewing this policy.

The designated governor, who is also the Data Protection Officer, checks that the school complies with this policy by, among other things, reviewing school records.

This document will be reviewed at least every two years, if there is a significant change in the law or in official guidance on the implementation of the law, and following the implementation of the General Data Protection Regulation.

At every review, the policy will be shared with the governing board.

13. Links with other policies

This Information Security Policy is linked to:

- the Freedom of Information Publication Scheme
- the Privacy Notices described above
- the Data Protection Policy
- the Data Retention Policy
- the CCTV Policy

These documents, which may be updated from time to time by the School, are available on the School's website or upon request to the Data Protection Officer, Zia Rehman.