ROYAL HIGH SCHOOL
BATH

GDST

GDPR – INFORMATION SECURITY [JAMES MOYLE] 2021-22

This policy has not required changes as a result of the Covid-19 Crisis.

Applicable to: All staff, governors, students and parents.

Objective

The aim of this policy is to protect the confidentiality, integrity and availability of our information assets, whether in paper or digital form in order to:

- safeguard and promote the welfare of our students
- support our students' learning and help every student fulfil her potential
- support students with Special Educational Needs or Disability (SEND)
- communicate with our network of alumnae
- manage our schools effectively
- manage the employment of our staff

Procedure

Information Security is defined as the preservation of:

- **Confidentiality**: ensuring information is accessible only to those authorised to have access;
- **Integrity**: safeguarding the accuracy and completeness of information by protecting against unauthorised modification; and
- **Availability**: ensuring information and services are available to authorised users when required.

Legal and Regulatory Requirements

All staff have an obligation to ensure all information systems, information assets and users comply relevant legislation, including:

- Computer Misuse Act 1990;
- General Data Protection Regulation 2016;
- Payment Card Industry Data Security Standard;
- Privacy and Electronic Communications Regulation 2003

Note: If you are unsure about the relevant legal or regulatory requirements relating to the information you use in your work, or suspect there may have been a breach of any regulations or the law please contact the Data Protection Officer or legal team for guidance.

If you believe there may have been a breach of the confidentiality, Integrity or Availability of any information system, a vulnerability to any security controls, or a breach of IT policies and procedures please report this to the Data Protection officer.

Information Security Controls

Information security controls are used to help mitigate risk. These controls are divided into administrative, technical and physical categories:

Administrative Controls

Accountabilities and responsibilities
All staff are responsible for ensuring any personal information they hold is kept securely and reasonable precautions are taken against physical loss, damage or unauthorised disclosure. In certain circumstances it may be a criminal offence to disclose personal data to third parties without authority. All staff should ensure that:

- any personal data they hold is kept securely
- Personal information is not disclosed orally, in writing or transferred by electronic means to any unauthorised person.
- Personal information held on any digital media storage device is stored in encrypted format and password protected

There is a statutory presumption in the UK that material created by an employee during the course of employment is generally owned by the employer. This may be referred to as Intellectual Property, or IP. If a member of staff wishes to retain copies of any work produced during the course of their employment after leaving the GDST they may only do so if this has been authorised in advance by their line manager.

Staff are not authorised to retain the personal information of students, parents or staff beyond their period of employment and this material and must return any documents containing student, parent or staff personal information to the school, or permanently delete them from any personal records or media storage devices at the conclusion of their employment.

All authorised users of the GDST's IT equipment and systems have responsibilities to protect information assets and comply with information security procedures. However, some staff have special responsibilities for maintaining information security:

Information Asset Owners (IAO)

An information asset is *a body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited effectively* and an information asset owner is *a senior/responsible individuals involved in running the relevant business area.*

Information assets within schools are likely to include pupil records, financial information, building maintenance information and employee records

Information asset owners are responsible for the information assets within their areas of business, ensuring appropriate controls are implemented, recognising actual or potential security incidents and ensuring that policies and procedures are followed. Information asset owners may assign responsibility for maintaining the accuracy of databases to a database administrator.

While Head teachers remain responsible for the confidentiality, integrity and availability of all information and assets, the role of IAO may be delegated to an appropriate member of staff.

Senior Management Team

SLT members at schools and the SMT at Trust Office have overall accountability and responsibility for understanding and addressing information risk within their own business areas and for assigning ownership for information assets to Information Asset Owners.

Director of ITS

The Director of ITS is responsible for implementing an appropriate Network Security strategy across the GDST and has overall responsibility for the development, management and maintenance of all of the GDST's IT and communications infrastructure, equipment, systems, processes and procedures.

Data Protection Officer (DPO)

Responsible for informing and advising the organisation and its employees about their obligations in complying with Data Protection laws, for monitoring compliance, advising on Data Protection Impact Assessments and training. The DPO is the first point of contact for supervisory authorities.

Database Administrator

Responsible for maintaining the integrity of the data on a database system (for example SIMS).

Network Manager

Responsible for the delivery of IT services within schools. They are responsible for purchasing and installing local IT equipment in line with the wider GDST Network security strategy and standardisation policy, and for maintaining their school computers, servers, switches and networks.

System Administrator

This is the description of a role assigned to a member of IT staff with technical skills and qualifications. System administrators are responsible for the configuration and operation of a computer or IT system. Administrator access ordinarily provides complete control of a system or application and is performed by IT technical experts. Servers and computers on the GDST IT network use administrator and Local User accounts. Administrator accounts provide full access to files, directories, and can be used to change access control permissions and download software onto devices attached to the GDST network.

General Users

Are provided with a local user account with rights and permissions assigned according to their need.

Super User

Super users are also general users, but they may have specialist knowledge on a particular system or application, for example CPOMS. Super users may be involved in the delivery of training, or the creation of local user accounts within an application.

Information Classification

Different types of information require different security measures depending on their sensitivity, and we must ensure sensitive information is protected against unauthorised access, disclosure or modification. Further information on the GDST Information classification Standard may be found on The Hub.

Disposal of paper records

Paper records that contain confidential, restricted, or personal information must be disposed of by shredding, or via a secure disposal service provider. For the disposal of equipment containing confidential, restricted, or personal information, please refer the GDST Asset Management and Data Sanitisation procedure which may be found on The Hub.

Acceptable Use of IT equipment and systems

There are different versions of the GDST IT acceptable use agreement for staff, senior and prep students. Copies of these acceptable use agreements can be found on The Hub. Users of GDST IT systems must accept and sign an 'Acceptable Use Agreement' before access to equipment and systems is granted.

Data Protection

The GDST Data Protection policy accompanies this policy in the School Policies and is also available on The Hub.

Personal Data Breaches

'Personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. Further information on our data breach reporting procedure can be found on The Hub.

Technical Controls

Network Security

The Director of IT is responsible for implementing an appropriate Network Security strategy across the GDST.

Note: The GDST has adopted the UK Government Cyber Essentials scheme, together with the National Cyber Security Centre '10 Steps to Cyber Security' as baselines for our Cyber Security risk assessments.

Cyber Incident Response Procedure

The National Cyber Security Centre defines a cyber-incident as a breach of a system's security in order to affect its integrity or availability and/or the unauthorised access or attempted access to a system or systems; in line with the Computer Misuse Act (1990).

If any member of staff suspects a cyber-incident may have occurred, or is being attempted they should notify a member of the IT team immediately.

The member of the IT team should assess the information, apply initial containment actions as appropriate and urgently escalate the matter to the Director of ITS (or their deputy)

Further information on the Cyber Incident Response Procedure may be found on The Hub.

Network Attached Devices

Staff and students are not permitted to connect any computer or electronic device to the primary GDST network, or install software onto a GDST computer without prior approval from IT Services.

Note: A 'guest network' is available for staff and students to connect personal devices.

Disk Image Deployment

In order to provide a unified foundation for all desktops and laptops across the GDST, and to ensure we operate on the same operating system version

- the ITS team at Trust Office are responsible for providing an up to date disk image through the Microsoft System Centre Configuration Manager (SCCM).
- Network Managers are responsible for using this disk image when deploying or re-imaging Microsoft devices

Local Administrator Accounts

Servers and computers on the GDST IT network use administrator and Local User accounts. All staff are provided with a local user account with rights and permissions assigned according to their need.

Administrator accounts provide full access to files and directories, and can be used to change access control permissions and download software onto devices attached to the GDST network. To ensure our network is secure and appropriate controls are in place to restrict access to sensitive information it is necessary to restrict administrator access to IT specialists.
All Administrator accounts must comply with the GDST Local Administrator Standard. Further information on this standard may be found on The Hub.

Passwords

Each user is responsible for the security of their passwords. Further information concerning the GDST password policy can be found on The Hub.

Multi factor authentication

Two factor authentication (MFA) provides an additional layer of security when using a system or application containing sensitive information. MFA ordinarily involves the use of something a user knows (a password) together with something a user has (a token, biometrics or mobile phone).

Functions within the GDST where MFA are considered appropriate include system administration access and 'authorizers' of finance systems.

Role based access control

With role based access control security is managed at a level that corresponds with the GDST organisational structure. Users are assigned one or more roles, and each role is assigned one or more privileges that are permitted to users in that role. Security administration consists of determining the operations that must be executed by persons in particular jobs, and assigning employees to the proper roles

Note: Security administration is performed by system administrators and may not be performed by employees who perform tasks within that system.

The principle of least privilege (POLP)

The principle of least privilege is the practice of limiting access rights for users to the bare minimum permissions they need to perform their work. Under POLP, users are granted permission to read, write or execute files or resources with the least amount of privilege necessary to do their job

Federated identity management (FIM)

Identity federation links a user's identity across multiple security domains, each supporting its own identity management system. When two domains are federated, the user can authenticate to one domain and then access resources in the other domain without having to perform a separate login process.

IT Disaster Recovery Plan and business continuity

The GDST Backup highlights the responsibility of system owners to backup critical data. Further information is provided on The Hub.

Privacy by Design

Privacy by Design describes the principle of implementing appropriate technical and organisational controls at the point of designing a solution in order to protect the rights and freedoms of data subjects.

A Privacy by Design approach must always be adopted. Where the processing of personal data presents a high risk to the rights of data subjects, a Data Protection Impact Assessment (DPIA) must be undertaken. When completing a DPIA advice should be sought from the DPO

Security penetration testing

An annual IT health check will be performed by an independent third party approved by 'Crest' or 'Check'. This health check comprises penetration tests to search for vulnerabilities within the IT infrastructure and is performed both within the corporate network and from outside. This simulates the processes an IT hacker would deploy to try and break into the GDST's secure environment.

Any issues arising from the health reported to the Director of IT and SIRO who (where appropriate) are jointly responsible for producing a remediation plan.

Anti Virus controls

The Director of IT is responsible for developing and monitoring anti-virus measures, to protect the GDST from computer virus infections and other malicious programs.
Network Managers are responsible for ensuring that;

- All of their systems are up to date with the latest version of the AV client software
- All AV software is running with the latest DAT file (containing AV signatures)
- An active AV scan is undertaken every week

Patch management

As vulnerabilities are identified in software supporting computer systems, including routers, firewalls, servers, and operating systems, companies release a 'patch' (coding update). Hackers may seek to exploit known vulnerabilities in an effort to breach network security and 99.9% of attacks happen due to commonly used exploits and commonly found vulnerabilities existing in companies' systems that have not yet been patched.

When a vendor stops supporting software they will no longer release patches for discovered vulnerabilities. When new loopholes come to light, they will remain vulnerable as patches will not be released to fix them

- IT managers are responsible for ensuring their systems are up to date with all patches released by vendors within 14 days of the patch being released.
- Devices with unsupported software must not be connected to the GDST network or the public internet.

Data Encryption

All devices capable of storing personal data must be deployed with encryption enabled. Where it is not possible to encrypt the device memory (i.e. a camera memory card) and additional layer of physical security must be used, for example by storing the device in a locked cupboard, drawer or office.

Portable memory devices

An endpoint security solution will be deployed to protect and encrypt any portable memory device connected to the GDST network

Payment Card Industry Data Security Standard (PCIDSS)

The PCIDSS is a scheme operated by the Payment Card Industry on behalf payment card companies (for example Mastercard). The scheme ensures that merchants (including the GDST) securely protect card holder data when taking card payments. This includes the environment in which card holder data is collected and processed. Compliance with PCI-DSS is a mandatory requirement of the merchant agreement the GDST has with its bank. Further information on the GDST PCIDSS procedure may be found on The Hub.

Physical Controls

Physical Access controls

The GDST Health and Safety strategy employs a number of measures including physical access controls to protect IT assets, prevent unauthorised access to GDST premises, and prevent access to personal or confidential information. Further information on our Health and Safety security strategy can be found on The Hub.

Clear Desks

All staff are required to ensure that all confidential or restricted information in hardcopy or electronic form is kept secure, in particular;

- Computer workstations must be 'locked' when a workspace is unsupervised.
- Any Confidential or Restricted information must be removed from desks and locked in a drawer or filing cabinet when the desk is unoccupied and at the end of the work day.
- Filing cabinets containing Restricted or Sensitive information must be kept closed and locked when not in use or when not supervised.

Server room security

It is the responsibility of IT Services to ensure that appropriate security controls are in place for the server room. The server room is a restricted area and access must be restricted to IT staff by way of additional physical security such as a locked door.

IT asset management and data sanitisation

IT assets often hold sensitive personal information relating to staff and students and IT Services are responsible for maintaining a database of all IT assets. This describes the assets, who they are allocated to and records any authorised uses and security procedures related to them. IT assets must be allocated to an individual, who has use of and is responsible for them.

Data must be sanitised from IT assets in the following circumstances;

- **Re-use:** When a device is being reallocated to a different user
- **Repair:** When a faulty device is sent to a third party for repair
- **Return:** at the conclusion of a period of lease or loan
- **Destruction:** when the device is being disposed of

Further information on the GDST asset management procedure may be found on The Hub.

Review: September 2021	**Next Review:** June 2022