SUTTON COLDFIELD GRAMMAR SCHOOL FOR GIRLS

IT POLICY

Date: May 2023

Revision Date: July 2025

Created By: Matt Moody (IT Systems Lead)

Contents

Background

The Sutton Coldfield Grammar School for Girls (referred to as SCGSG within this document) IT Support Department aims to support the development of communication and information tools, systems for research, learning and management within the school and between the school and a variety of stakeholders. This policy is intended to facilitate the smooth and consistent running of systems and services in support of this aim.

The term "Information and Communications Technology" (ICT) can be interchanged with the term "Information Technology" (IT) in much current documentation, this policy uses the term IT. Most of the tools of communication and information technologies: audio, video, telephones, mobile devices, photocopiers, printers, computers and network infrastructure are included in the department's remit. This broad definition of "IT" has been used throughout the policies and should be kept in mind when interpreting them.

Typographic convention: *italicized text* indicates explanatory notes rather than policy.

A. SCHOOL POLICY STATEMENT

A.1 Scope of IT Policies

SCGSG IT policy and its supporting policies apply to:

1. All staff and students within the school and all other users authorised by the school, whether at school premises or elsewhere. *This includes visitors to the school from other organisations (Please see Appendix 2).*
2. Users from other institutions under arrangements covered by location independent networking (LIN).
3. The use of school-owned, on-loan facilities. They also apply to all private systems whether owned, leased, rented or on-loan when connected to the school's network directly or indirectly.
4. All school-owned or licensed data/programs, be they on school systems or private systems, and to all data/programs provided to the school by sponsors or external agencies.

The IT systems covered include servers, workstations, desktop computers, laptop/notebook/handheld computers, communications equipment, photocopiers, telephones, mobile devices and audio visual equipment installed anywhere within the school, or operated on behalf of the school at another location.

This policy is to be used in conjunction with AUP (Acceptable Use Policy), which has to be signed by all students and staff when they join the school.

A.2 Objectives

The objectives of IT policy and its supporting policies are to:

1. Provide systems that are suited to their purpose.
2. Provide and maintain safe IT equipment in a suitable environment, and to ensure safe working practice in the operation of IT equipment.
3. Ensure that the school achieves best value in its IT provision.
4. Ensure that school's IT facilities are adequately secured.

5. Ensure that users are aware of and fully comply with the relevant legislation, policies, procedures, guidelines and standards.
6. Ensure safe, and socially and environmentally responsible disposal of equipment in line with the current Waste Electrical and Electronic Equipment Recycling (WEEE) regulations;
7. Ensure that the school plays an active and responsible part in the wider education community in its use of information technology.
8. Ensure that all students, as children, are safeguarded as much as possible against external threats using appropriate technologies and instruction through appropriate school and DfE recommended practice.

Definitions of terms used in this Policy Statement can be found in Appendix 1.

A.3 Responsibilities for IT Policies

The IT Systems Leader and the Senior Leadership Team (SLT) have responsibility for:

- initiating and drafting IT policies and for delegating the production of supporting documentation.
- arranging the consultation process and approval as appropriate for each policy.
- maintaining IT policies in an up-to-date and accessible form.
- arranging the dissemination of IT policies in an appropriate and accessible way.

It is the responsibility of each individual, defined in paragraph A.1 above, to ensure their understanding of and compliance with this and associated policies. Such responsibility is part of a member of staff's contract of employment and a student's Acceptable Use Agreement (AUP). All other users are required to sign the agreement in Appendix 2 when necessary.

A.4 Compliance with Legislation

SCGSG has an obligation to abide by all relevant legislation. This policy and supporting policies, procedures, guidelines and standards must satisfy all applicable legislation. This obligation formally devolves to all users defined in A.1 above, who may be held personally liable for any breach of the legislation.

If anyone finds an inconsistency between policies and legislation, or between individual policies, they must bring this to the attention of the IT Systems Leader, IT Network Manager or any member of the SLT as soon as possible.

A.5 Health and Safety

SCGSG will provide and maintain equipment that is safe in the context of its intended use. Individual users have a responsibility to operate these systems safely and report any defects. Managers with responsibility for health and safety should follow recognised guidelines in assessing risk, and should consult the Facilities and Compliance Manager when advice is needed.

All users must follow manufacturer’s instructions or handbooks in the installation and operation of IT systems, and should consult the Facilities and Compliance Manager when advice is needed.

A.6 Environmental responsibility

All systems within the scope of this policy will be acquired, operated and disposed of in an environmentally responsible manner and in line with the WEEE regulations.

A.7 Policy Awareness

All IT policies and guidelines will be made freely available electronically on the school website to everyone to whom they apply (see A.1 above) and these will form the up-to-date official version. Policies and guidelines will also be published in the staff appointment pack, Student Journal and contractors' guidelines. Copies will also be made available on paper if this is required.

Anyone responsible for authorising the use of facilities within the scope of this policy and its supporting policies is responsible for informing new users of IT policies.

All IT procedures and standards will be published electronically wherever possible, however where publication could compromise safety or security, procedures and standards will be restricted.

A.8 Changes to IT Policies

The normal process for changing IT Policies will be for a request to be made to the IT Systems Leader and in some cases, the SLT, who will arrange for suitable approval from the relevant Governing Board committee. At this point the published IT Policies will change.

In the event of a need for urgent change, this may be approved by the IT Systems Leader and implemented immediately, pending formal approval from the SLT and Governing Board. Any urgent changes will be published immediately with the changes highlighted as provisional.

A.9 Status of IT Policies

It is a condition of employment that staff will abide by SCGSG Rules and Policies, of which IT Policies are an essential part. Where a member of staff does not abide by these, then dependent on the severity of the misconduct, the Governing Board, Headteacher, or a senior member of staff (when delegated to), will deal with incident in accordance to the SCGSG disciplinary policy and procedures.

The school's rules and policies, including IT policies, are an integral part of the students' experience at SCGSG.

IT policies are an integral part of the school's policies, to which contractors must adhere.

B. COMPLIANCE WITH LEGISLATION.

B.1 Introduction

Users must comply with current British legislation in all respects when using IT systems and equipment. Some of the legislation and guidance, which applies particularly to these circumstances is:

- Data Protection Act 2018
- The UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020
- Computer Misuse Act 1990
- Human Rights Act 1998

- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Regulation of Investigatory Powers Act 2000
- Education Act 2011
- Freedom of Information Act 2000
- Education and Inspections Act 2006
- Keeping Children Safe in Education
- Searching, screening and confiscation: advice for schools 2022
- National Cyber Security Centre (NCSC): Cyber Security for Schools
- Education and Training (Welfare of Children) Act 2021
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Meeting digital and technology standards in schools and colleges

Data Protection Act and General Data Protection Regulation

Users must comply with the school's GDPR Data Protection Policy as published on the school website.

Intellectual Property Right, Licenses etc.

No user may copy programs or information to paper, removable media (such as USB hard drive or flash drive), non-removable media (such as hard disk) or to portable devices, except where explicitly allowed by the license agreement/contract and where no copyright or intellectual property right is infringed.

Theft and misuse

Unauthorised removal of school-owned, leased, rented or loaned IT equipment, software or data from the school's premises constitutes a theft.

No user may interfere with protection systems. *This includes: any device which is provided to prevent removal or theft of equipment; any software or configuration that detects or prevents virus infection; any software or configuration that prevents the running of non-approved software.*

No user may install or use software or systems which are not licensed for use.

SCGSG systems may not be used to transmit, store or access text, images, recordings, scripts, programs or telephone calls that contain:

- Material likely to contravene current legislation such as sexist, racist, homophobic, xenophobic, transphobic, pornographic, paedophilic or discriminatory material, except in the legitimate pursuit of valid pre-authorised research authorised by the IT Systems Leader or Headteacher in delegation with the Governing Board.
- Text, images or recordings to which a third party hold copyright or other intellectual property right, without the written permission of the right holder.
- Material that is defamatory, libellous, slanderous or threatening.
- Material that could be used to breach computer security or to facilitate unauthorised entry into computer systems.
- Material that is likely to prejudice or seriously impede the course of justice in UK criminal or civil proceedings;
- Material containing personal data as defined by the Data Protection Act 2018 and/or GDPR, unless the subjects' permission has been explicitly given in writing.

The Regulation of Investigatory Powers Act 2000

SCGSG's systems may intercept any communication transmitted across or stored on its systems provided that this is within the framework of the Regulation of Investigatory Powers Act 2000 (RIPA). In particular, it may monitor but not record communications:

1. To anonymous helplines.
2. To determine whether communications are for personal or business purposes, except where personal use contravenes the staff conduct policy.

The school may monitor and record communications for the following purposes:

- To ensure that users are complying with policies, conditions of use, procedures and guidelines and with British legislation, or AUP.
- To monitor standards of quality, performance and security.
- To prevent or detect crime.
- To investigate unauthorised use of systems.

When an external agency requests information under the RIPA Act, the Headteacher or another member of the SLT will be the point of contact. In their absence, the IT Systems Leader or IT Network Manager shall be the point of contact.

SCGSG routinely logs transactions on its systems. This logging covers the transmission of e-mails, access to web pages, the placement of telephone and logging in and out of user network accounts. Some administrative systems also have transaction logging enabled. Electronically recorded messages and logs may be automatically backed up; these backups will also be covered by the RIPA Act.

All other interceptions must be authorised by the IT Systems Leader responsible for the system on which the interception is to take place. In this person's absence, responsibility will be assumed by the IT Network Manager, who liaise with a relevant member of SLT. The IT Systems Leader will act as the compliance officer and is responsible for ensuring that policies and procedures are implemented in accordance with the RIPA Act.

Accessibility

Where electronic information is provided with the intention of being generally accessible, this information should be in a suitable form for those with disabilities to gain access to the information wherever practicable. *This particularly applies to information on the World Wide Web where internationally recognised Accessibility Guidelines should be used when authoring material.*

The school will, wherever possible, make suitable provision for legitimate users with disabilities to access relevant information using appropriate information technology.

B2. Conditions of Use for IT Systems

Principles

SCGSG IT assets must be safeguarded, operated and administered in the best interests of the school and its community. The interests of individuals or sections should not override the requirements for provision and continuity of service for the remainder of the school.

Access to equipment and information

Only those within the scope of the IT Policy, A.1, may use SCGSG IT systems.

No user may read/view/listen to, modify or delete any file or information without authorisation from the owner of the file. SCGSG reserves the right to remove material from its systems, which it deems to be unsuitable. Criteria for suitability are given later in this section. Removal of material may be governed by the **GDPR Data Protection Policy** or this policy. Where this is not applicable, the authority is vested in the IT Systems Leader or IT Network Manager. *Where information is clearly provided for other users to access (such as on the Internet or intranet), authorisation to read/view/listen to is implicit.*

Shared access to file space must be managed through the use of operating system services. It is not normally permitted for users to allow someone else to log in under their username in order to make use of their file space or for any other purpose. If temporary access needs to be given to someone else, the usual practice would be for the normal user to perform the login process. If, for legitimate operational or training reasons and with the approval of the IT Network Manager, IT Systems Leader or Headteacher, a password is divulged to someone else, the password must be changed as soon as possible. *See below:* security of passwords.

A user must login to a shared system only under a username which they have been allocated. Logging in to a machine using someone else's username, password or PIN number is an offence unless it is for legitimate operational or training reasons and with the approval of the IT Network Manager or higher authority. *The Headteacher or other member of the senior leadership team may consider it necessary to access an absent member of staff's files or email messages in order to maintain continuity of service. Where the absent member of staff's password is not known, the IT Support Department should be contacted in order to gain access. However, procedures should not normally require a user seeking assistance to divulge his or her password to anyone else.*

Security of passwords and PIN numbers

In order to use school systems, both staff and student users are required to have a long password that does not follow easily guessable patterns (such as the use of “Password” or containing any part of that person’s name or computer username/email address).

The guidance and advice which directs this password policy is generally derived from the school’s primary source of IT security information – the National Cyber Security Centre (NCSC). An example of their current advice may be found:

- https://www.ncsc.gov.uk/collection/passwords
- https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online

At present staff and student users are treated differently. Staff users have more stringent controls than student users due to the level of access to sensitive information that they have.

As an example, all new staff members must implement multi-factor authentication (MFA) for remote access to Microsoft 365 applications. This is supported by information on password strategy in their mandatory TES Educare online training and IT induction training.

Controls in use within school are:

- Minimum password length (12 characters, no maximum).
- Complexity requirements (where common passwords are also barred from use).

- Last 3 passwords remembered.
- Passwords not stored with reversable encryption.
- Failed attempt lockout (5 attempts, within 10 minutes).

All staff are required to complete the required NCSC Cyber Security Training annually as part of our RPA insurance requirements. Staff are also required to repeat the TES Educare Cyber Security and Digital Resilience training every 3 years.

Encryption

All electronic communication outside of the school will be encrypted automatically by the school's mail server. Users are obliged to ensure that if they are sending what could be classed as confidential information that they follow best-practice and separately encrypt any files that leave the school. Where possible this transfer will be performed by secure transfer sites to ensure individuals' data is protected.

SCGSG-owned devices are encrypted using TPM (Trusted Platform Module) technology.

External devices (such as USB flash drives or external USB hard drives) used by staff will need to be encrypted before data may be transferred from the SCGSG network, though this is not encouraged.

Use and security of equipment and information

IT resources are only available to users as defined in policy A.1. Additionally, the resources must have been allocated and/or approved by SCGSG for their use.

IT resources may only be used for the purpose they are intended and in the way these systems are configured. Only SCGSG-appointed IT Support staff, approved contractors or others with approval from the IT Systems Leader are permitted to change the use or system configuration of SCGSG IT equipment and software. Users are permitted to change user preferences to suit their working practice or style provided the settings do not compromise security or alter operability for others.

No user may use a computer system in any way which puts files or information belonging to someone else at risk of damage. In particular, knowingly introducing a computer virus is a serious offence which may result in disciplinary or even legal action where appropriate.

Users must cooperate with the IT Support Department in preventative or remedial action concerning equipment and data security.

Publishing, or communicating without the authority of either the IT Systems Leader or Headteacher of any information which allows someone else to breach the security of the computer systems is an offence. *Examples are user's passwords or loopholes in system security which a user may come across accidentally whilst making legitimate use of the facilities. All users must inform the IT Support Department when they find evidence of failures or weaknesses in security. The IT Systems Leader and IT Network Manager have the authority to give information which allows a breach of security, but this would normally be confined to testing and detection purposes only.*

When requested to do so by the staff or other responsible persons, anyone using SCGSG communication and information technology equipment must be prepared to identify themself by presenting their SCGSG-issued identity card.

Users are required to treat IT equipment with care, other users and IT Support Department staff courteously.

SCGSG access to the Internet is governed by respective Acceptable Use Policies (AUPs), which allows for education, research and institution business. All users must comply with this policy.

SCGSG systems may not be used to transmit, store or access text, images, recordings, scripts, programs or telephone calls that:

1. Will consume sufficient network or server resource as to impede the effective use of systems by other users.
2. Is likely to incur unwarranted costs on the school.
3. Is likely to involve users or staff in wasted time.
4. Contain misleadingly out-of-date information.
5. Contain inaccurate or deceiving information.
6. Seeks to unreasonably trivialise, insult or degrade other individuals, groups or bodies, or infringe others' human rights.
7. Use techniques that capture or otherwise display third party information is such a way as to give the impression that they come from anywhere other than the original source.

The IT Systems Leader and other authorised staff can read any file stored on the system and, if it is necessary to safeguard the integrity of the system, to delete any file without warning.

B3. School IT Security Policy

Scope and Purpose

The purpose of this policy is to ensure the availability, confidentiality and integrity of IT systems which support the academic and administrative activities of the school. Effective security is achieved by working with a proper discipline, in compliance with legislation and SCGSG policies, and by adherence to approved procedures and standards.

Objectives

The objectives of this policy are to:

- Ensure that SCGSG IT facilities are adequately protected against loss, misuse or abuse.
- Raise awareness of IT security issues throughout the school and to ensure that they are considered at every stage of an IT system life cycle.
- Ensure that users understand their responsibilities for protecting the data they handle.

Responsibilities for Information Systems Security

The IT Systems Leader, IT Network Manager and SLT are responsible for implementation of this policy and related projects.

Proposals for IT Projects should be made to the IT Systems Leader.

The IT Systems Leader and IT Network Manager have the authority to take any action in the event of an IT emergency deemed necessary to protect the school's systems and information within the scope of this policy.

Protection from cyber attacks

The school will ensure that best-practice measures are in place to protect the IT systems and data safe from cyber attack. These measures, although not exhaustive include:

- Compliance and membership of the RPA Cyber Attack insurance scheme. This includes:
  - Offline backups
  - Staff competition of NCSC Cyber Security training video
  - Registration with Police CyberAlarm
  - An active Cyber Response Plan
- Annual accreditation of the school's systems and procedures against the ISAME Cyber Security Essentials scheme.
- Regular review of compliance against the DfE "Meeting Digital and Technology Standards in Schools and Colleges" document. (https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/cyber-security-standards-for-schools-and-colleges)
- Staff must complete the online training for Cyber Security and Digital Resilience within the first 12 months of their employment. This will be repeated every 3 years.
- Regular backup testing (at least once per month) that is logged.
- Regular review of IT software and hardware to ensure security patches are applied and/or systems are replaced with newer/more secure variants.

Compliance with Legislation

The school has an obligation to abide by all relevant legislation. This policy and supporting policies, procedures and standards satisfy the requirement under the Data Protection Act 2018 and GDPR for a formal statement of the school's security arrangements for personal data. The requirement formally devolves to all users defined in Policy A.1 above, who may be held personally liable for any breach of the legislation.

Risk Assessment and Security Review

Individual users have a responsibility to identify the value of the systems and information under their control and to make provisions for their safety.

Provision of Network Services

The IT Systems Leader is responsible for authorising standard and non-standard services on the SCGSG network.

B4. Policy for Use of Information Servers

An Information Server is classified a web server, VLE or Portal, which must have an owner who is authorised by the IT Network Manager or IT Systems Leader.

The Information Server Owner (ISO) is responsible for compliance with all relevant school policies and current legislation. *This makes the ISO responsible to different people or groups for their actions, for example, to the Data Protection Officer for compliance with Data Protection legislation, to the IT Systems Leader for network function, for audit availability and to users for the quality of the data.*

Each ISO is responsible for the availability, accountability, authenticity, confidentiality, integrity and reliability of their systems and data.

The ISO will assess the value to the school of the information served, identify threats to that information and arrange safeguards which are commensurate with the identified risk.

The ISO is responsible for monitoring changes to the value of information, or the threats to it and making appropriate changes to the safeguards.

The ISO will regularly review the operation of the above safeguards to identify attempts to compromise the server. All "successful" compromises must be reported immediately to the local IT Support Department. All attempts, whether successful or not, should be reported to the IT Network Manager or IT Systems Leader.

The ISO will take all possible precautions to ensure that system does not interfere with the operation of any of the school's IT systems.

Information Servers must be available at any time for a security audit by SCGSG's IT Support Department or auditors.

The ISO must ensure that it is possible to disconnect the server immediately at all times.

B5. Equipment and Software used by groups and/or individuals

The following policies apply to equipment and software which is used by an individual or shared by a group of users and are additional to the Acceptable Use Policy (AUP) and other appropriate policies. *Examples of equipment to which this policy applies are telephone handsets, AV equipment, desktop and laptop computers, individual and shared printers, photocopiers/MFDs.*

Specification and selection of IT equipment must be done by or in consultation with the IT Support Department.

Purchase of equipment and software must be in accordance with the finance guidelines for the school.

The IT Support Department will maintain a record of the current location of IT equipment. Movement of normally fixed equipment should be supervised by a member of the IT Support Department wherever possible. Where this is not possible, the IT Support Department should be notified of all changes.

The IT Support Department will maintain a record of all software license purchases. *All software purchases and valid license must be presented to the IT Support Department before installation on to the school's network.*

Installation and upgrading of individual and workgroup equipment and software will be undertaken by the IT Support Department or an approved contractor.

No user may install additional hardware, software or alter the configuration of any equipment except:

1. IT Support Department staff and other authorised personnel may install hardware, software or alter equipment configuration for testing and evaluation.
2. Where hardware or software has been procured via the IT Support Department and is accompanied by adequate instructions for installation, the hardware or software may, by mutual agreement, be given to the user for them to install. This shall be deemed as authorisation to install only this item.

3. Auto-updating software (e.g. virus signature files) originally installed and configured by the IT Support Department may continue to install updates under the authority of the IT Support Department.
4. Periodic updates to software may be undertaken by a member of staff provided the member of staff has adequate instructions, appropriate skill and legitimate access to the equipment involved.
5. If hardware or software, other than updates to existing software, is to be acquired by a member of staff, other than via the IT Support Department (e.g. by personal purchase or download from the Internet), the member of staff must consult with a member of the IT Support Department for known issues concerning that hardware or software.
6. Portable computers belonging to users or their employers may be connected to the SCGSG network, provided that the software is adequately patched and it is protected from infection by malicious software and from transmitting malicious software to other systems. Notes of Guidance for connecting to the school's network will be available but no support for non-SCGSG equipment will be provided by the school. Non-SCGSG users, such as those from other institutions using location independent networking (LIN), must operate within the IT Policy and at the discretion of the IT Network Manager or IT Systems Leader.

Any installation will ensure that data is backed up before adding additional hardware or software.

No license agreement may be entered into if the consequences or potential consequences will adversely affect performance or incur direct or indirect costs on the school unless authorised by the IT Systems Leader.

All installations and upgrades must be within the terms of the license agreement and must be deleted in accordance with the license.

Every user must ensure the correct use and adequate safeguarding of data for which they are responsible. This includes suitable backups of the data.

No equipment may be used to serve information except where authorisation from the IT Systems Leader has been gained. *Examples of serving information include creating a Web or ftp server; allowing other computers to connect to your computer or obtain remote access.*

All portable equipment and software shall have a designated user. The designated user is the person with whom the equipment is normally lodged and this person is responsible for the security of the equipment and software. The designated user, the designated user's line manager, and the IT Support Department have the ability to authorise the use of that portable equipment and software outside of the school's premises.

Equipment on temporary loan must be recorded in the relevant equipment log as being on loan to a named individual who will be responsible for the security, correct operation and condition of the equipment, and for its return in good condition within the agree period of the loan. In some cases, the loan will authorise the individual to remove the equipment from SCGSG premises for the period of the loan. Failure to return the equipment by the end of the loan period will be considered as theft.

No equipment may be taken off SCGSG premises (unless covered by a loan agreement) without the permission of the IT Systems Leader or IT Network Manager.

The IT Support Department may make arrangements for the temporary provision of equipment to individuals or workgroups. Temporary provision of equipment to a student will only be made

with written authorisation from the student's Head of Year, SENCO or Senior Leader. This equipment is available on a first come, first served basis.

All redundant equipment and software must be passed to the IT Support Department for redeployment or for disposal in accordance with 'WEEE' regulations.

B6. Maintenance and support of IT equipment and software

Resources for the maintenance and support of IT equipment and software will be managed based on the needs of the school. Priority will be given to maintenance and support of equipment and software that is widespread or critical in nature. Lower priority will be given where equipment or software is older, less widespread or non-critical to the school or its general operation.

The IT Support Department provides maintenance and support for IT equipment and software if it is owned, licenced or leased by SCGSG.

The school will designate information storage formats and media that it supports. Older formats that were supported will have an obsolescence period during which the format will no longer be actively used but can be transferred to a supported format.

B7. Connection to and from accounts on SCGSG Systems

Connections to the school network

Only approved equipment may be connected to or used to access the SCGSG network. *In particular, no wireless access points may be connected to the school's network without approval.* Approval is given by the IT Systems Leader.

Operating procedures and conditions for all connected equipment must be approved by the IT Systems Leader.

Connection of equipment to the SCGSG network shall only be performed by staff from the IT Support Department or approved contractors, except that:

- Users may connect their own or their employer's device to the network provided they follow the latest guidelines available from the IT Support Department.
- All equipment connected to the SCGSG network must be registered with the IT Support Department either prior to, or for the purpose of, connection. Network configuration and registration information about the network is maintained centrally by the IT Support Department.

Remote access to the SCGSG network

Remote access for users to the school's network will normally be via the Internet using a secure user "portal" and or VPN. For details of these servers, contact the IT Support Department. Users are responsible for their own equipment and connection outside the school's premises.

The school will not provide or maintain external connections into the SCGSG network except where an approved contractor or service requires a dial-up link for the purposes of maintaining specific systems or services. Such connections must be set up and maintained in accordance with procedures agreed with the IT Systems Leader or IT Network Manager.

No user may set up or maintain a private connection into the school's IT resources.

Approved services

Only approved services may be used on the SCGSG network. Current approved services are determined by the IT Systems Leader.

Accounts on the network

All staff, whether full-time, part-time, permanent or temporary, academic guests and enrolled students may have an account on the SCGSG network. Temporary accounts for academic purposes may be obtained when a request is supported by a member of the SLT, IT Network Manager or IT Systems Leader. Requests must be made to the IT Support Department.

Staff who retire but continue their academic association with the school may retain their account on the network. Periodic checks will be made on the use of the account and the account will be expired in accordance with policy when the account is no longer in use.

Every account will be set as "expired" when a member of staff's contract is ended in SIMS.Net (MIS Software) and no later than four months after the account holder leaves the employment of the school. *An "expired" account remains on the system and will process email messages. It will not allow the account holder access to the school's systems.*

Every account will be deleted no earlier than 6 months and no later than 12 months after the account holder leaves SCGSG, unless disciplinary or investigative circumstances warrant a different course of action or that member of staff was a Senior Leader or SENDCO. *When an account is deleted, the contents of all network directories (including email directories) associated with the account will also be archived in the first instance and deleted after a maximum period of 12 months.*

Staff account holders may have a grace period exceeding these limits in on request to and at the discretion of the IT Support Department.

B8. Use of electronic communication systems (including E-Mail and Microsoft Teams)

SCGSG electronic communication systems are provided for the conduct of school-related business. Incidental and personal use is permitted so long as such use does not disrupt or distract the individual from school business (due to volume, frequency or time expended), does not incur unreasonable cost to the school, and/or does not restrict the use of those systems to other legitimate users. *Users are reminded that the school can access their communications for operational and security purposes.*

A user's account will be assigned and named by the relevant SCGSG address/format policy.

The facility to alias an account is available to all users on request to the IT Network Manager or IT Systems Leader. Domain names will not be aliased. Aliases must be unique and will be allocated on a first-come first-served basis. Aliases must be non-trivial and must comply with SCGSG policies as decided by the IT Systems Leader, who has the right to refuse an alias request.

Contact e-mail addresses for sections of the school will be provided by an alias, shared mailbox or separate account, on request to the IT Network Manager or IT Systems Leader.

Anonymous accounts for users will not be allowed on SCGSG systems. *Anonymous accounts do not allow proper management, accountability or traceability and would inherently contravene IT policies.*

Essential information may be provided to users using electronic communication channels. Users are responsible for reading and responding as appropriate within the time limit specified in the message subject.

Trade Union representatives and members may use SCGSG systems for related Trade Union communications.

SCGSG network and communication systems may not be used to transmit:

- Material unrelated to school business, including bulk e-mail transmissions (SPAM).
- Messages requesting the recipient to continue forwarding the message to others, where the message has no educational or school-relevant value.
- Messages with forged addresses (spoofing) or otherwise purporting to come from a source other than the true sender.

SCGSG will provide the following classifications of distribution list:

- Staff classification lists. (e.g. Non-Teaching Staff, Teaching Staff, SLT)
- Class groups. (for staff-student messaging)
- Year groups. (for staff-student messaging)
- Subject groups. (for staff-staff messaging)
- Staff initiative groups. (such as Quality Assurance, Enrichment, Trip Leaders)

Communication channels and their operation will be regulated by the IT Systems Leader.

The school will designate and regulate distribution lists. Users cannot opt out of these lists. *Core announce lists are used as essential communication mechanisms between SCGSG and users, so it is important that the school regulates their membership.*

B9. Use of the Internet

Access to the Internet (Web) is provided for research, teaching, learning and other legitimate school-related business. Incidental and personal use of the Internet is permitted so long as such use does not disrupt or distract the individual from school business (due to volume, frequency or time expended), does not incur unreasonable cost to the school, and/or does not restrict the use of those systems to other legitimate users.

Website pages published using SCGSG systems must comply with the policy for Information Servers and the data protection guidance set out in our **GDPR Data Protection Policy**.

It is the responsibility of the member of staff authoring the pages to comply with SCGSG policies regarding content, presentation, accessibility, data protection and security.

Pages containing dynamic content must have the involvement of the IT Systems Leader, IT Network Manager or Marketing and Digital Communications Assistant in their development and approval for their compliance with policies. "*Dynamic content" means that the page's content may change either by user interaction or by changes in the source data used in the page. Examples of dynamic pages are: pages that rely on an element of programming for their content; pages that accept input from users; pages that use a database as their source of information.*

Students will not have access to public space, in-house web space provision will be provided by the IT Support Department.

Only users allocated by the IT Systems Leader, IT Network Manager or Marketing and Digital Communications Assistant may have access to the school's web sites, control panel and content management pages.

B10. Use of Telephones

The telephone systems provided by SCGSG are provided for research, educational and other legitimate business. Incidental and personal use of the telephones is permitted so long as such use does not disrupt or distract the individual from school business (due to volume, frequency or time expended), does not incur unreasonable cost to the school, and/or does not restrict the use of those systems to other legitimate users. *Short calls of a personal nature that are required as a result of changed school circumstances (such as having to work late at short notice) are considered to be in support of school-related business and may be legitimately made. Users wishing to make private calls should normally do so using a personal mobile phone.*

Where exceptional personal circumstances may lead to infringement of this policy, users should agree with their line manager the acceptability of their telephone usage.

Each school-provided mobile phone shall have a registered user and that user will be responsible for the use and security of the phone. The registered user must report the loss of or any damage to their phone to the IT Systems Leader, IT Network Manager or the Finance and Operations Director.

Where technically possible and no cost is incurred, individuals should retain their existing internal telephone number when moving to another location within school. Where this is not possible or an additional charge is associated with the provision, this will be agreed with the IT Systems Leader or Finance and Operations Director.

Trade Union representatives and members may use SCGSG telephone systems for school-related Trade Union communications.

B11. Use of photocopying and printing equipment

SCGSG provides photocopiers and printers for research, educational and other legitimate school-related business. Incidental and personal use of photocopiers and printers is permitted so long as such use does not disrupt or distract the individual from school business (due to volume, frequency or time expended), does not incur unreasonable cost to the school, and/or does not restrict the use of those systems to other legitimate users. *In practice copying and printing will incur a cost to the school, however the school provides facilities for payment for copier and printer charges, and these should be used when appropriate.*

The school will monitor the charges for all photocopying and networked printing. Any waivers will be agreed by the IT Systems Leader or Finance and Operations Director.

B12. IT Purchasing Policy

SCGSG's Tendering and Procurement Policy will be followed in the purchase or lease of IT Equipment.

All procurement of IT equipment, software and services for the school must be made either through the IT Support Department or in full consultation with the relevant personnel in the IT Support Department. The IT Support Department may veto a purchase or lease if it believes that IT policies have been breached.

Where a non-IT Support Department budget is being used to fund a purchase or lease, it is the budget-holder's responsibility to ensure that sufficient funds are available for the purchase and that all relevant information is supplied to the IT Support Department to facilitate the purchase/lease.

Where existing suppliers make favourable arrangements available to staff or students for equipment or software purchase, these discounts will be made available either directly between supplier and individual or via the IT Support Department. In the latter case, the school reserves the right to apply a charge to cover administration costs.

B13. Disposal of IT Equipment

All equipment will be disposed of in compliance with current legislation and with due regard for social and environmental considerations.

Disposal shall not expose the school to continuing commitment to support or maintain any systems.

Disposal of equipment shall constitute best value to the school.

Where equipment has no residual value, recycling of materials or components shall be done in as economical a way as possible.

B14. The Community beyond SCGSG

SCGSG will play a responsible role in the UK academic community in support of information technology by participating in and contributing informally to appropriate networks of contacts.

SCGSG should maintain formal membership of appropriate organisations in support of IT and its application in the academic community.

B15. Non-compliance with these policies

Illegal Activities

Infringements of the relevant legislation, summarised in Section B1, will result in legal and/or disciplinary action. All such infringements must be reported to the IT Systems Leader or SLT, who have the authority to deal with minor breaches and to escalate more serious offences.

Breaches of School Policies

Correcting problems caused by a breach of IT policies will be done at minimum effort and cost to the school. SCGSG reserves the right to pass on some or all of the cost involved to those causing the breach.

Consequences of violations of SCGSG IT Policies will depend on the intent, the seriousness of the offence and the damage caused. All such violations must be reported to the IT Systems Leader or SLT, who have the authority to deal with minor breaches and to escalate more serious offences.

IT Support Department staff, with authorisation from the IT Systems Leader, may disconnect equipment without notice if it is believed that IT Policies are breached while an appropriate investigation is carried out.

Breach of Policies by students may result in:

1. Suspension of access to IT equipment and services for minor breaches.
2. Formal disciplinary action, which may result in suspension or permanent exclusion from school, for more serious offences.

Breach of Policies by staff may result in:

1. Suspension of access to IT equipment and services for minor breaches.
2. Formal disciplinary action for more serious offences.

Redress

If any user believes that the action taken by SCGSG is disproportionate to the alleged breach of policy, they may appeal through the School's Grievance Procedure.

Appendix 1 – Definition of Terms Used

Accountability - The property that ensures that the actions of an entity may be traced uniquely to the entity. (ISO 7498-2: 1989) e.g. an audit log in a database server.

Distribution lists - E-mail lists that send a single message to multiple users. Only designated editors may send to an Announce list.

Authenticity - The property that ensures that the identity of a subject or resource is the one claimed. Examples of infringement include impersonation and IP spoofing.

Availability - The property of being accessible and usable upon demand by an authorised entity (ISO 7498-2:1989)

Confidentiality - The property that information is not made available or disclosed to unauthorised individuals, entities or processes (ISO 7498-2: 1989)

Information Server - Any computer system which may be used to store and make available information. The information may be text, images, video and sound and examples of server systems include Web, E-mail, VLE, Database, Portal and FTP. Networking equipment is also considered to fall within this definition: routers, switches and hubs. The system may be operated by employees of the school or by a third party on behalf of SCGSG.

Integrity - Data Integrity is the property that data has not been altered or destroyed in an unauthorised manner (ISO 7498-2: 1989), and System Integrity is the property that a system performs its intended function free from deliberate or accidental unauthorised manipulation.

Private discussion lists - E-mail lists that allow members to send a message to a list and that message gets sent to all members of that list. One person controls the list of recipients, the list is therefore "private" rather than "open" for anyone to subscribe.

Private Information - Any information which has not been officially approved by a relevant SCGSG staff body or local governing body committee.

Reliability - Consistent, intended behaviour and results.

School Information - Information officially approved by a relevant party committee.

School-related business - Any activity or function that directly or indirectly supports or contributes to SCGSG's core business of education.

User - Any person authorised to use SCGSG IT systems including staff, students, visitors and contractors.

Appendix 2 – Agreements and Disclaimers

Staff Acceptable Use Policy (AUP)

In order to allow you to use the school's IT System; including computer equipment, video-conferencing, teleconferencing equipment, software, network(s), and Internet access; the following Acceptable Use Policies have been established:

1. SCGSG dedicates the property comprising of the network and grants access to it by users only for the educational activities authorised under the school's policies and procedures.
2. The Member of Staff agrees not to use any part of the school's systems to harm or disrupt other people, their work, any network, hardware, software, or data.
3. The Member of Staff will not knowingly send, install, or create a computer virus or use the school's systems in a way that violates the IT policy.
4. The Member of Staff will keep their username and password confidential and will not reveal it to others.
5. The Member of Staff understands and agrees that their electronic communications (e.g. e-mail) and/or data on any SCGSG computer or media is not private and that the school has access to all mail and other data, including internet logs. These may be reviewed by the school at any time.
6. The Member of Staff may not use the school's systems for financial gain or to support or oppose political candidates, groups, or ballot measures.
7. The Member of Staff will not access, submit, publish, display, and/or install on or through the school's systems any defamatory, harassing, obscene, sexually explicit, threatening, or illegal material or other material that is disruptive to the educational environment.
8. The Member of Staff will not use the school's systems to encourage use of alcohol/controlled substances or violence against others or access sites that do so.
9. The Member of Staff will treat the files of others as private and will not access anyone's folders, work, or files without that person's permission.
10. The Member of Staff will not attempt to use another person's login or password.
11. The Member of Staff understands and consents to the fact that actions taken on or through the network may be recorded and replayed, including, but not limited to, audio and video recordings through teleconferencing, videoconferencing, and/or creation of multimedia projects.
12. The Member of Staff will not install any software on SCGSG equipment, any software required must be authorised and installed by the IT Support Department only.
13. The Member of Staff will not install or transmit copyrighted material through the school's systems illegally.
14. The Member of Staff will not attempt to bypass any of the filtering or security software. When accessing other networks or systems through the school's systems, the Member of Staff will abide by all rules of that network or system.
15. The Member of Staff is aware that some sites accessible may contain defamatory, inaccurate, abusive, obscene, sexually oriented, threatening, offensive, or illegal material and the Member of Staff understands that SCGSG does not condone the use of such materials. Members of Staff should be aware that the filtering software used by the school is not infallible and that users may be able to access inappropriate materials. In the event any material is accessed, the IT Support Department must be notified immediately.

16. The Member of Staff understands and agrees that use of SCGSG's systems is at their own risk and SCGSG is not liable for harm suffered by any party as a result of using the school's systems.
17. The Member of Staff agrees to be accountable for their actions. If the Member of Staff intentionally or recklessly inflicts any damage or harm on any portion of the school's systems or to any party through the school's systems, the Member of Staff may be subject to discipline and restitution. If the Member of Staff observes other users violating these terms and conditions, violators will be reported to a member of the Senior Leadership Team or IT Support Department.
18. The Member of Staff may not use the school's systems to participate in any activities that violate UK laws, school policies, or these terms and conditions. The Member of Staff will abide by all terms listed in the SCGSG IT Policy.
19. Attaching network-capable equipment to the network, unless authorised by the IT Systems Leader or IT Network Manager, is strictly prohibited.
20. It is your responsibility to ensure that if you are to connect any SCGSG equipment to your home broadband connection, that it is adequately protected. For example, ensure that any wireless connection is encrypted using WEP or WPA encryption.

I have read and understand the SCGSG Staff Acceptable Use Policy.			
Staff Signature:		Date:	
Print Name:		Department:	

Student Acceptable Use Policy (AUP)

In order to allow you to use the school's IT Systems; including computer equipment, video conferencing/ teleconferencing equipment, software, network(s), and Internet access; the following Acceptable Use Policies have been established:

The school dedicates the property comprising of the network and grants access to it by users only for the educational activities authorised under the school's policy and procedures;

1. The student agrees not to use any part of the school's IT systems to harm or disrupt other people, their work, any network, hardware, software, or data. The student will not knowingly send, install, or create a computer virus or use the school's IT system in a way that violates the school's policy;
2. The student will keep their username and password confidential and will not reveal it to others;
3. The student understands and agrees that their electronic communications (e.g. e-mail) and/or data on any school computers or media is not private and that the school has access to all mail and other data, including internet logs, and these may be reviewed by the school at any time;
4. The student may not use the school's system for financial gain or to support or oppose political candidates, groups, or ballot measures;
5. The student will not access, submit, publish, display, and/or install on or through the school's system any defamatory, bullying, harassing, obscene, sexually explicit, threatening, or illegal material or other material that is disruptive to the educational environment;
6. The student will not use the school's system to encourage use of alcohol/controlled substances or violence against others or access sites that do so;
7. The student will treat the files of others as private and will not access anyone's folders, work, or files without that person's permission;
8. The student will not attempt to use another person's username or password;
9. The student understands and consents to the fact that actions taken on or through the network may be recorded and replayed, including, but not limited to, audio and video recordings through teleconferencing, videoconferencing, and/or creation of multimedia projects;
10. The student agrees not to install any software on school's equipment;
11. The student will not install or transmit copyrighted material through the school's system illegally;
12. The student will not attempt to bypass any of the school's filtering or security software. When accessing other networks or systems through the school's system the student will abide by all rules of that network or system;
13. The student and parent are aware that some sites accessible through the school's system may contain defamatory, inaccurate, abusive, obscene, sexually oriented, threatening, offensive, or illegal material and the student and parent understand that Sutton Coldfield Grammar School for Girls does not condone the use of such materials. Parents of minors should be aware that the filtering software used by the school is not infallible and that users may be able to access inappropriate materials. In the event any material is accessed, a member of staff must be notified immediately;
14. The student understands that the school has the right to reformat any system's drives and/or remove/relocate any given data or computer at any time and is not responsible for any loss of data;

15. The student understands and agrees that use of the school's system is at their own risk and the school is not liable for harm suffered by any party as a result of using the school's system;
16. The student agrees to be accountable for their actions. If the student intentionally or recklessly inflicts any damage or harm on any portion of the school's system or to any party through the school's system, the student will be subject to discipline and restitution. If the student observes other students violating these terms and conditions, violators will be reported to a member of the school's staff;
17. The student may not use the school's system to participate in any activities that violate UK laws, school policies, or these terms and conditions. The student will abide by all terms. A copy of which is available on request;
18. Any network-capable equipment attached to the school's network, unless authorised by the IT Network Manager or IT Systems Leader, is strictly prohibited;
19. It is your responsibility to ensure that if you are to connect any school equipment to your home broadband connection that it is adequately secured and protected. For example, ensure that any wireless connection is encrypted using WEP or WPA encryption.

I have read and understand the SCGSG Student Acceptable Use Policy.			
Child's Signature:		Date:	
Parent/Carer's Signature:		Date:	

Manufacturer:	
Laptop Model:	
Serial Number:	
Network Name:	
Staff Name:	

Staff Device Loan Agreement

This device will be **loaned** to you while you remain employed by SCGSG.

Please indicate your acceptance of the conditions below by signing one copy of this form and returning it to the IT Support Department.

Whilst the device is in your care the following conditions should be noted:

1. The device **remains the property of the school** and is only for the use of the person to which it is issued. The device should not be loaned to other individuals (e.g. family members or friends).
2. Insurance cover provides protection from the standard risks but excludes accidental damage and theft outside of the school's premises. For example, if the laptop is stolen from an unattended vehicle, you (or your own insurance) will be responsible for the cost of its replacement.
3. Only software licensed by the school or authorised by the IT Systems Leader or IT Network Manager, which is installed by a member of the school's IT Support Department may be used. Under no circumstance should you install any software yourself.
4. Anti-Virus software is installed and must be updated on a regular basis. The device must be connected to the Internet (ideally the school network) at least once per week to allow itself to update and report back.
5. **In the event of a problem, do not attempt to repair the device or have it repaired yourself.** The device must be returned to the IT Support Department, who will take appropriate action.
6. Any charges incurred by accessing the Internet from outside the school are not chargeable to the school.
7. School policies regarding appropriate use, data protection, computer misuse and health and safety must be adhered to by all users of the device.
8. You must return the device to the IT Support Department in good condition, before you leave the school, or at the request of the IT Support department staff. If you fail to do so, you agree to pay for its replacement. The school will invoice you for the full cost of its replacement.
9. If we ask you to return the device to the school for any reason, **you must do so**. You will be given reasonable notice of this.
10. Sutton Coldfield Grammar School for Girls is not responsible for the purchase of peripheral devices (printers etc.), software, consumables or internet costs from home.
11. The device MUST be kept in the bag/sleeve/case provided when not in use.

12. Any breach of this agreement *could* result in the cessation of the equipment loan and/or disciplinary action.

Manufacturer:

Laptop Model:

Serial Number:

Network Name:

Staff Name:

Collected by staff:

Signature.....Date.....

Returned to:

Technician.....Date.....

Receipt of laptop S/N (Serial Here) return:

Signature.....Date.....

Technician.....Date.....

Manufacturer:
Laptop Model:
Serial Number:
Network Name:
Name of Student:

Student Device Loan Agreement

This laptop will be *loaned* to you while you remain at the school.

Please indicate your acceptance of the conditions below by signing one copy of this form and returning it to the IT Support Department.

While the laptop is in your care the following conditions should be noted:

1. The Laptop **remains the property of Sutton Coldfield Grammar School for Girls** and is only for the use of the student to which it is issued. The laptop should not be loaned to other individuals (e.g. family members, friends or other students).
2. Insurance cover provides protection from the standard risks but excludes accidental damage and theft outside of the school's premises. For example, if the laptop is stolen from an unattended vehicle, you (or your parents'/carers' insurance) will be responsible for the cost of its replacement.
3. Only software licensed by the school or authorised by the IT Systems Leader or IT Network Manager, which is installed by a member of the school's IT Support Department may be used. Under no circumstance should you install any software yourself.
4. Anti-Virus software is installed and must be updated on a regular basis. The device must be connected to the Internet (ideally the school network) at least once per week to allow itself to update and report back.
5. **In the event of a problem, do not attempt to repair the computer or have it repaired yourself.** The computer must be returned to the IT Support Department, who will take appropriate action.
6. Any charges incurred by students accessing the Internet offsite are not chargeable to the school.
7. School policies regarding appropriate use, data protection, computer misuse and health and safety must be adhered to by all users of the laptop.
8. You must return the laptop to the IT Support Department, in good condition, before you leave the school or at the request of the IT Support department staff. If you fail to do so you (or your parent/carer) agrees to pay for its replacement. The school will invoice your parent/carer for the full cost of its replacement.
9. If we ask you to return the laptop to the school for any reason, **you must do so**. You will be given reasonable notice of this.
10. The school is not responsible for the purchase of peripheral devices (printers etc.), software, consumables or internet costs from home.
11. The laptop MUST be kept in the bag provided when not in use.
12. If your laptop is damaged in **any way**, for example, a broken display and the IT Support Department assesses that this is the not the result of normal wear and tear then you will

be liable for a **minimum repair charge of £50.00**. In exceptional circumstances this may be increased due to the level of damage.

13. Any breach of this agreement could result in the cancellation of the equipment loan and/or appropriate sanctions in line with the school's behaviour policy.

Manufacturer:

Laptop Model:

Serial Number:

Network Name:

Name of Student:

Collected by parent/carer/student:

Signature.....Date.....

Returned to:

Technician.....Date.....

Receipt of laptop S/N (Serial Here) return:

Signature.....Date.....

Technician.....Date.....

Email Disclaimer Used

DISCLAIMER - This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. If you have received this email in error please notify itsupport@suttcold.bham.sch.uk and remove it from your system. Please note that any views or opinions presented in this email are solely those of the author and do not

necessarily represent those of the school. The recipient should check this email and any attachments for the presence of viruses. Sutton Coldfield Grammar School for Girls accepts no liability for any damage caused by any virus transmitted by this email.

IT Monitoring Statement

*(visible to all users **before** logon screen on network-managed computers)*

By continuing to use this device, you agree to abide by the school's IT Policy and Acceptable Use Policy (AUP). You also accept that the school's systems are actively monitored for security and safeguarding purposes.

Irresponsible use may result in the loss of Internet or systems access.

Network access must be made via the user's authorised account and password, which must not be given to any other person.

School computer and Internet use must be appropriate to the student's education or staff professional activity.

Copyright and intellectual property rights must be respected.

Electronic communications (e.g. E-Mail or Microsoft Teams messages) should be written carefully and politely, particularly as messages may be forwarded or printed and be seen by unexpected and external readers.

Users are responsible for electronic communications they send and for contacts made.

Use for personal financial gain, gambling, political purposes or advertising is not permitted.

INITIAL EQUALITY IMPACT ASSESSMENT FORM

Name of policy/activity/project:

IT Policy

Is this a new or an existing policy/activity/project?

Rewrite of new policy

Scope/timescales for project or activity (including review date):

Approval in June 2023, next in 2025.

Policy/project lead and Author of Equality Impact Assessment:

Finance and Operations Director

Outline of main aims of this activity/policy/project:

To ensure secure IT Systems.

Who will benefit/be affected by this policy/activity?

Students, staff, Trustees and parents of Sutton Coldfield Grammar School for Girls and also visitors to the Trust.

If an existing policy/activity, do you have any data of use by or impact on different groups which may raise concerns over an equality impact?

No concerns

Does the activity have the potential to impact differently on groups due to a protected characteristic (eg race/ethnicity, gender, transgender, disability, religion & belief, age, sexual orientation, maternity/paternity) for:

No.

(a) Students and members of the community? (eg The Governing Board, students, contractors, visitors, hirers of the premises, agency staff, suppliers etc). Which groups are likely to be affected?

No

(b) Employees?

No

Does this activity make a positive contribution to the Trust's general or specific duties under the Equality Act 2010? If yes, please detail.

Yes – the Policy applies to all equally

Having reviewed the potential impact of the policy/activity listed above, **I believe a full impact assessment is required / NOT required** (delete as applicable with justification below)

Full impact assessment is not required

Justification: The policy is of equal benefit to all students, regardless of gender, race, religion, sexual orientation etc.

Name : Doug Thorp Date : May 2023