Queen Elizabeth's School
INFORMATION AND COMMUNICATION TECHNOLOGY POLICY

INTRODUCTION

Queen Elizabeth's School depends on Information and Communication Technology (ICT) services for its teaching, learning and administrative activities. These services are provided on condition they are used for legitimate, authorised purposes, and the School may be required from time to time to demonstrate to external auditing bodies that it has mechanisms in place to manage, regulate and control them.

The safeguarding of pupils is a primary concern with respect to the use of ICT, with the School committed to protecting young people from online harm. Further details on online safety are included in the School's Safeguarding (Child Protection) Policy.

SCOPE OF THE POLICY

This Policy applies to all staff and pupils and all other computer, network or information users authorised by the School. It covers the use of all ICT services and telephone facilities provided by the School or by third parties on behalf of the School. More particularly, the Policy relates to staff and pupils' use of any School-owned facilities (and those leased by or rented to the School), centrally managed or otherwise; to all private systems (whether owned, leased, rented or on loan) when connected to the School network; to all School-owned or licensed data and programs; and to all data and programs provided to the School by sponsors or external agencies.

Pupils are explicitly bound to abide by the School's regulations, of which this document forms a part. Staff are also obliged to abide by this Policy as a condition of their employment. If a user is not sure whether something they intend to do might contravene the rules on ICT use, they should check first with their Line Manager (in the case of staff) or their Form Tutor (in the case of pupils).

In all cases, the act of using the School's ICT systems implies acceptance of the conditions of use and compliance with regulations and relevant Acts of Parliament.

From time to time, the School may issue good practice guidelines, and it reserves the right to withdraw network services that are not operated in accordance with those guidelines.

1. AUTHORISED USE

The aim of this section is to define what constitutes acceptable use; to encourage the responsible use of facilities; to maximise the availability of resources (equipment, infrastructure and staff) for legitimate purposes; and to minimise the risk of misuse from inside or outside of the School.

i. Definition

"Authorised use" is defined as:

- *For pupils*: Use properly associated with the School's programme of study for which a student is registered; and reasonable personal use;

- *For staff*: Use in the course of or properly and directly associated with their employment; and reasonable personal use.

Reasonable personal use is defined as incidental and occasional use which does not:

i) Disrupt or distract the individual from the efficient conduct of School business (i.e. due to volume, frequency, time expended or time of day used);
ii) Involve accessing, downloading, storing or sending offensive or inappropriate material or information, or is such as to amount to a criminal or civil offence;
iii) Restrict the use of those systems by other legitimate users;
iv) Risk bringing the School into disrepute or placing the School in a position of liability;
v) Add significantly to running costs; and
vi) Breach any School policy, including without limitation the Bullying and Equal Opportunities Policies.

ii. Regulations

Users must:

i) Respect the copyright of all materials and software that are made available by the School's service providers and third parties for authorised use;
Users must not make, run or use unlicensed copies of software or data. They should only download data or datasets where they are explicitly permitted to do so. They must abide by the CHEST Code Of Conduct For The Use Of Software Or Datasets: http://www.eduserv.org.uk/services/Chest-Agreements/about-chest*); the terms of the JISC Model Licences (see* http://www.jisc.ac.uk/publications/programmerelated/2009/scaiprtoolkit/2modellicence.aspx*); copyright law (Copyright, Designs and Patents Act 1988) (as amended) and by any specific conditions of use imposed by the owners or suppliers of software or data. In particular, users should be aware that, unless otherwise stated, software and datasets provided by the School should only be used for School educational purposes.*

ii) Comply with the requirements of data protection law, including the UK General Data Protection Regulation and the Data Protection Act 2018;
Data Protection laws protect individuals against the unauthorised use or disclosure of their data. The School is registered with the UK Data Protection authorities. The processing, misuse or disclosure of an individual's data outside the School's registration may amount to a criminal offence.

iii) Comply with the *Computer Misuse Act 1990* which makes activities such as hacking or the deliberate introduction of viruses a criminal offence;
Hacking is defined here as the unauthorised use of a computer system (locally or through a network), or the use of resources that have not been allocated, with intent to access, modify or damage another's files or system files, or to deny service to legitimate users, or to obtain or alter financial or administrative records, or to facilitate a crime.

iv) Take all reasonable precautions to prevent the introduction of any virus, worm, Trojan Horse or other harmful program to any computer device, file or software; including by accepting all software updates (on mobile devices), unless otherwise advised by the School.

v) Perform routine housekeeping of their emails, voicemails and electronic files stored on School computers and devices;

vi) Take account of the School's Safeguarding Policy when overseeing, and dealing with, any use of electronic media

vii) Abide by the terms and conditions, as set out upon receipt, of any device issued or loaned via the School;

viii) Securely store and transport any School device (hardware) issued and report immediately to IT the loss or theft of any such School device, any damage sustained to it or any fault which occurs, requiring attention; and

ix) Report immediately to the Headmaster and Data Protection Officer any circumstance in which you suspect personal data has been disclosed, knowingly or in error, to an unauthorised person or persons.

Users must not:

i) Use material or programs in a way which is unlawful, defamatory or invasive of another's privacy;

ii) Use the services and facilities in such a way as to risk or to cause loss, damage or destruction of data or breaches of confidentiality of data, including by submitting to unauthorised external 'cloud' storage providers any personal, confidential or school sensitive information or data (the School will however promote the use of authorised cloud-based systems e.g. via Microsoft 365);

iii) Use the services and facilities in a way which infringes any patent, trademark, trade secret, copyright, moral right, confidential information or other proprietary right of any third party;

iv) Access or process personal data for any purpose beyond that which it was intended upon collection, or in any way which otherwise breaches the School's Data Protection Policy, such as sharing data with unauthorised third parties;

v) Jeopardise the provision of services (for example, by inappropriate use of bulk email, by recreational use that deprives other users of resources, or by actions which interfere with the conduct of online learning/remote education);

vi) Publish, create, store, download, distribute, transmit, or intentionally access material that is offensive, obscene, indecent or unlawful;
Such materials will always include, but at the School's discretion may not be limited to, items deemed to be offensive, obscene, indecent or unlawful with regard to the Obscene Publications Act 1959 (as amended), Race Relations Act 1976 (as amended), Equality Act 2010, Part-Time Workers (Prevention of Less Favourable Treatment) Regulations 2000, Fixed-Term Employees (Prevention of Less Favourable Treatment) Regulations 2002, Protection from Harassment Act 1997, Protection of Children Act 1978 (as amended), Public Order Act 1986 (as amended), Criminal Justice and Public Order Act 1994 (as amended), Terrorism Act 2006 and the Counter-Terrorism and Security Act 2015.

vii) Use ICT facilities in a way that brings or could bring the School into disrepute. This includes associating the School with external facilities such as websites that could bring the School into disrepute by association, for example, by embedding the School email addresses in such sites;

viii) Disclose passwords to others, or use accounts or passwords belonging to others, or otherwise to circumvent registration procedures;

ix) Access or attempt to access computers or computing services at the School or elsewhere for which permission has not been granted, or facilitate such unauthorised access by others;

x) Attempt to circumvent, deactivate or uninstall any firewall, software or device management solution designed to protect systems against harm, or to protect information on a loaned or issued device in the event that it is lost or stolen;

xi) Interfere or attempt to interfere with or destroy systems or software set up on public facilities (this includes loading or attempting to load unauthorised software on to any School ICT facilities or devices);

xii) Interfere with, disconnect, damage or remove without authority any equipment made available for use in conjunction with any School ICT facilities; and

xiii) Set up equipment to provide services that they are not competent to administer, especially if such services result in security vulnerability or exposure to misuse.

The School does not tolerate discrimination or harassment in any form whatsoever. This principle extends to any information distributed via any School system or via the internet. Users may not store on or transmit from any system any material which discriminates or encourages discrimination or harassment on grounds of gender, sexual orientation, gender reassignment, marital or civil partner status, age, race, ethnic origin, colour, nationality, religion, belief or disability (characteristics protected under the Equality Act 2010).

Failure to comply with these regulations may lead to disciplinary action, up to and including dismissal without notice (staff) or permanent exclusion (pupils) from the School, and may expose an individual to court proceedings attracting both criminal and civil liability. Any person contravening these regulations will be held responsible for any claims brought against the School and any legal action to which the School is, or might be, exposed as a result of their unauthorised use.

In the event that a member of staff or pupil receives or becomes aware of obscene, indecent, offensive, inflammatory, discriminatory or socially offensive material, or material they believe could indicate affiliation or vulnerability to any form of extremism, fanaticism or radicalisation, they should notify a senior leader (in the case of staff) or their Form Tutor or Head of Year (in the case of pupils).

iii. Conditions of Use

Use of School ICT facilities is subject to the following conditions:

i) The School accepts no liability for any loss (including any loss of software, data or other computer functionality or any economic, consequential or indirect loss), or damage (including damage to hardware, software or data or the invalidation of any warranty agreement) to equipment not owned by the School as a consequence of any work carried out on such equipment by members of staff (or pupils acting in the capacity of members of staff), whether authorised or not;

ii) The School accepts no liability for any loss (including any loss of software, data or other computer functionality or any economic, consequential or indirect loss), or damage (including damage to hardware, software or data or invalidation of any warranty agreement) to equipment not owned by the School as a consequence of direct or indirect connection, whether authorised or not, to School networks;

iii) The user shall indemnify the School for any loss or damage, whether direct or indirect, malicious or inadvertent, suffered or incurred by the School as a consequence of the interconnection of any hardware or software not owned by or under the control of the School with any ICT system, hardware, software or data owned or controlled by the School;

iv) Any charges incurred by accessing the internet out of School or via the purchase of apps and their associated add-ons on loaned devices are not chargeable to the School;

v) The School reserves the right to inspect, monitor, copy and/or remove user data in order to investigate operational problems or for the detection and investigation of suspected misuse. This includes the authorised interception and monitoring of communications as provided for by the *Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000*, made under the *Regulation of Investigatory Powers Act 2000 (as amended)*;

vi) For the avoidance of doubt, this does not preclude third parties who operate services on behalf of the School from carrying out lawful monitoring and disclosure on their systems and networks;

vii) The School reserves the right to check for insecure and vulnerable systems and to block access to systems and/or services which place at risk the integrity of its network or services, or which may pose a threat to third parties.

iv. Procedures for dealing with misuse or suspected security violations

i) Cases of misuse or abuse or actual or suspected security violations should be reported immediately to the School's Deputy Head (Operations). No attempt should be made to investigate security vulnerabilities unless or until appropriate authority has been obtained.

ii) In the event of suspected misuse of ICT facilities, the School reserves the right to suspend user accounts and to inspect, monitor, copy or remove users' files if necessary. The School may also disconnect network services and prevent access to the facilities without notice while investigations proceed.

iii) The Headmaster will be informed and will deal with the incident under the appropriate disciplinary procedures for pupils and staff. In some cases, legal action may be taken and the Police informed. The School reserves the right to disclose data or information about an individual's use of the School's computing facilities to any appropriate or authorised third party to assist in any further investigation, including as part of a referral to the anti-radicalisation Prevent or Channel programmes.

iv) Security breaches which could have resulted in the loss or unauthorised disclosure of personal data should also be reported to the School's Data Protection Officer, who may need to notify the Information Commissioner's Office.

2. EMAIL

Email is an important means of communication for the School and it provides an efficient method of conducting much of the School's business.

The Policy covers all School systems providing email services or any email service accessed from a School facility or any email service provided on behalf of the School. All users should treat emails from the School as formal correspondence.

The Policy affects all users of all such email services.

i. Appropriate use of School Email services

Use of email services is subject to all the same laws, regulations and codes of practice that apply to the use of other means of communication, such as telephones and paper records.

All pupils of the School and those staff whose duties require it, should have a School-provided email account which is to be used for email communications carried out on School business.

Users may not use School email services and/or facilities to transmit:

- Commercial material unrelated to the legitimate educational business of the School, including the transmission of unsolicited bulk email (spamming);
- Bulk non-commercial email which is likely to cause offence or inconvenience to those receiving it;
- Unsolicited email messages requesting other users, at the School or elsewhere, to continue forwarding such email messages to others, where those email messages have no educational or informational purpose (electronic chain letters);
- Email messages which purport to come from an individual other than the user actually sending the message, or with forged addresses (spoofing), other than where expressly authorised by the person in whose name the correspondence is being sent;
- Material which is offensive or inappropriate;
- Material which incites criminal activity;
- Material which may otherwise damage the School's teaching, learning, administrative or commercial activities;
- Material to which a third party holds an intellectual property right, without the express written permission of the rightholder;
- Material that is defamatory, libellous, harassing, threatening, discriminatory or illegal;
- Material that could be used in order to breach computer security, or 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; and
- Messages that could imply creation of an order or contract contrary to the School's procedures.

Caution should be exercised when drafting an email which references personal data. Encryption may be used to ensure confidentiality, but if there is any uncertainty about such email, advice should be sought from the School's Deputy Head (Operations) or the DPO (dpo@qebarnet.co.uk).

Whilst the School provides staff and pupils with access to email systems for the conduct of School-related business, incidental and occasional personal use of email is permitted provided such use does not disrupt or distract the individual from the conduct of School business (e.g. due to volume, frequency or time expended) or restrict the use of those systems for other legitimate users.

Users must not knowingly allow anyone else to send email using their accounts. Users will be deemed liable for any email or activity from their accounts.

Failure to comply with the terms of the Policy concerning email could result in access to the service being withdrawn or, in more serious cases, to disciplinary action being taken, and/or civil action and/or criminal prosecution.

ii. Viruses

All reasonable steps must be taken by all users to prevent the propagation of computer viruses by email. All desktop systems and mobile devices issued by the School (e.g. laptops/tablets) have anti-virus software installed and kept up to date, and incoming and outgoing email runs adequate virus detection software. Nonetheless, the effectiveness of the system relies additionally on the vigilance of email users, by, for example, being aware of rogue emails and leaving them unopened.

iii. Privacy and Security

Like all methods of communication, email cannot be assumed to be secure. It cannot be assumed that email will be correctly delivered or that the sender is as claimed in a mail header. Steps must be taken by users to minimise the risk of interception or breaches of confidentiality.

These steps include:

- Not divulging user passwords to anyone (including in email);
- Not knowingly allowing anyone else to send email from the user's account;
- The following guidelines should also be considered when sending emails:
  - Ensuring that the correct recipient email address is identified and used;
  - Considering anonymising references to specific individuals;
  - Confirming the identity of an email sender where there is reason to question this; and
  - Adopting a risk-based approach to deciding what information is appropriate to be sent by email.

Users should be aware that deletion of an email message by both sender and receiver does not mean that the message no longer exists on their systems or on the systems through which it passed. Conversely, when a message has been transmitted, it is not necessarily the case that a record of it will exist or be accessible.

Users may not, under any circumstances, monitor, intercept or browse other users' email messages.

Any personal electronic device, including laptops, tablets and mobile phones, holding mail messages, email addresses (or any other confidential material) relating to any aspect of School business should be protected by password, or other recognised and robust security authentication method (such as passcode, pattern, fingerprint or facial recognition). Users should log out of School email accounts when not in use.

iv. Investigating Email misuse

The School reserves the right to inspect, copy and/or remove user data in order to investigate operational problems or for the detection and investigation of suspected misuse of emails. This includes the authorised interception and monitoring of communications as provided for by the *Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000*, made under the *Regulation of Investigatory Powers Act 2000 (as amended)*.

The School reserves the right to access and disclose the contents of a user's email messages, in accordance with its legal and audit obligations, and for legitimate operational purposes. The School reserves the right to demand that encryption keys, where used, be made available so that it is able to fulfil its right of access to a user's emails in such circumstances.

Section 6 below gives further details about the monitoring of School systems and networks.

For the avoidance of doubt, this section does not preclude third parties who operate services on behalf of the School from carrying out lawful monitoring and disclosure on their systems and networks.

3. eQE

eQE is the School's e-learning platform and intranet and is used by all staff, pupils and parents. Guidance on acceptable use elsewhere in this Policy applies equally to this platform. Passwords should be kept secure and users will be accountable for the activity on their accounts.

No material which is illegal, obscene, offensive, derogatory, libellous, or in breach of copyright, should be posted to the platform, including to pages, on forums, or via the task and messaging services. eQE is for School business only, including teaching and learning, pastoral provision, enrichment activities, communicating operational information and for home-school communication. Staff and pupils interacting via eQE must do so professionally and in line with expectations in the Code of Conduct for Staf and Governors and the Pupil Discipline Policy.

Data supplied via eQE will be treated in accordance with the School's Data Protection Policy.

4. 1:1 DEVICE PROGRAMME

The School may arrange for the leasing of, or directly issue, personal IT devices (e.g. a laptop/tablet) to individual pupils and members of staff. The School's Digital Strategy includes plans to roll-out these 1:1 devices across at least Years 7-11. These devices are to enhance educational opportunities within the classroom, in structured extra-curricular enrichment activities and at home. The full provisions of this ICT Policy apply to the use of these devices.

The School's expectations and requirements for the use of these devices by pupils include that:

i) Payments are due monthly in advance via the Silverwing (Devices for Education) portal and are a condition of use. Those families deemed to require financial support will follow a different model which will be agreed directly with the School. Contact hmoffice@qebarnet.co.uk if you would like to discuss your financial situation in confidence.
ii) Pupils are required to look after their device when at home, when travelling to and from School, and when on School premises. Devices should be stowed safely in the case provided when not in use. Parents will be liable for charges to repair a device if it is broken due to lack of care.
iii) Devices must be charged at home, ready for use at School the following day. There is no facility to charge the device at School.
iv) Nothing must be downloaded on to the device which is not allowed by the School.
v) Devices must not have anything permanently attached to them, such as stickers or other decorations. Should a device be returned with such attachments at the end of the subscription period, the parents of the student concerned will be liable for the cost of that device.
vi) When the subscription period ends, the device must be returned to the School complete and in full working order, just as it was when originally provided, showing only normal wear & tear arising from proper use.

vii) At the end of the subscription period, the device must be returned with its original software and with all other hardware, including, but not limited to, charging cables, plugs and any official documentation pertaining to the device.
viii) In School, devices are only to be used as and when instructed by a member of staff.

5. SOCIAL MEDIA & INSTANT MESSAGING APPS

The aim of this section is to encourage responsible use of social media and to minimise the risk to staff, pupils and the School through the use of social media and instant messaging applications.

Social media in this Policy includes, but is not limited to:
i) Discord
ii) Facebook and Facebook Messenger;
iii) Flickr;
iv) Google+;
v) Instagram;
vi) LinkedIn;
vii) Pinterest;
viii) Snapchat;
ix) TikTok
x) Tumblr;
xi) Twitter;
xii) WhatsApp; and
xiii) YouTube.

i. Personal use of social media

Staff and pupils are permitted to make reasonable personal use of social media. The School strongly encourages all staff and pupils to do so within the bounds of the policies of the relevant services – such as age restrictions.

ii. Prohibited use of social media

Staff and pupils must not:
i) Use social media to breach School policies, including but not limited to the Staff and Pupil Disciplinary Policies (including the Code of Conduct for Staff and Governors), Bullying Policy, Equal Opportunities Policy and Data Protection Policy;
ii) Make any social media communications which could damage the School's interests or reputation, whether directly or indirectly;
iii) Use social media to defame the School, any staff, third parties associated with the School, pupils, parents or guardians;
iv) Impersonate any staff, third parties associated with the School, pupils, parents or guardians via social media;
v) Express opinions on behalf of the School using social media without express authorisation from the Headmaster;
vi) Use a School email address to set up a personal social media account, with the exception of a LinkedIn or QE Connect profile;
vii) Share confidential information relating to the School using social media; and
viii) Use School logos or images in any social media communications, or in their profile, without appropriate consent.

In addition, staff must not:

i) Make any social communications which could cause a conflict with their employment status or engagement with the School;
ii) Provide employment references for other individuals via social media;
iii) Contact or communicate with current or prospective School pupils via social media or instant messaging services unless clearly for the purpose of legitimate School business and there is no reasonable alternative method of communication e.g. in an emergency situation on a trip. Staff should exercise caution when contacting former pupils who have only recently left the School via social media, only communicating with them for professional purposes, for example in relation to upcoming School events or as part of the School's alumni relations and development work;
iv) 'Like' or share any images or posts of current School pupils on social media, other than where directly relevant to School business and professionally appropriate;
v) Accept requests from current School pupils sent to their personal social media accounts (with the exception of LinkedIn); and
vi) List their association with the School on their personal social media profile without expressly stating that they are sharing their own views.

iii. Acceptable use for School purposes

The School uses social media for business purposes. The use of social media in this manner is managed mainly by the Headmaster's office, although it may also be utilised by others for the purpose of generating support for the School from our alumni, or other partners, or appropriately celebrating school achievements.

Use of social media for School purposes is limited to:
i) Sharing non-confidential information such as the results of sporting events or recent success stories. The School will never disclose sensitive or confidential information via social media, without consent. Confidential information would include (but not be limited to) details of a pupil's exam results, family, address or other contact details, health or disability, religion or race, disciplinary matters etc.
ii) Providing updates in relation to School opening days and times, or important operational information;
iii) Posting non-confidential information of interest to staff, pupils, parents or guardians or the local community.

Any such postings must comply with other School policies, for example, the Safeguarding Policy, Equal Opportunities Policy and Data Protection Policy.

Staff and pupils must not set up social media sites or accounts in the name of the School without express approval from the Headmaster.

iv. Recruitment

The School may advertise vacancies using social media and carry out due diligence on job applicants during the recruitment process. This may include carrying out searches across staff's social media profiles. The School will still act in accordance with the School's Data Protection and Equal Opportunities Policies.

v. Misuse of social media

Failure to comply with the terms of the Policy concerning social media could result in disciplinary action being taken in accordance with the Staff Disciplinary and Pupil Discipline Policies.

6. MONITORING COMPUTER AND NETWORK USE

There are circumstances where the School may monitor or record communications made using its ICT systems, or examine material stored on those systems. The latter term is taken to include all components of the network as well as any other computer technology (whether or not they are owned by the School) attached to it.

It is important to be aware of the distinction made between:

i) Intercepting information **in transit:** Email messages being sent or monitoring web pages visited, for example. The relevant law is found in the *Regulation of Investigatory Powers Act 2000 (as amended)* and the *Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000*;
ii) Examination of material **stored** on a computer: The applicable law may vary according to variables such as who owns the computer, what material is being examined or how the material is examined.

Users should note that:

- Communications, including personal communications, made on or through the School's computing and telecommunications systems may be monitored or recorded to secure effective system operation and for other lawful purposes;

- Use of School systems is limited to authorised users only.

By using School systems, users accept that monitoring may take place.

i. The circumstances in which monitoring can occur

Provisions in the *Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000* permit the School to intercept and record information which can be associated with an individual's communications via School services (whether made for purposes associated with the School's business or activities or otherwise). This may be done in order to achieve the following aims:

- To safeguard users from inappropriate online content;
- To prevent or detect crime;
- To investigate or detect unauthorised use, including the use of systems outside the School;
- To ensure the effective and authorised operation of systems;
- To establish the existence of facts necessary to ascertain compliance with regulatory or self-regulatory procedures, or to ascertain or demonstrate standards;
- For other lawful purposes as set out in the relevant legislation.

Stored material (including email) may also be examined for these purposes. In addition, the School may access stored material in the event of an urgent need (see Section iii. below).

The School may also monitor but not record received communications to determine whether they are business or personal communications.

It should be noted that although reasonable personal use of facilities is permitted, excessive use that disrupts or distracts an individual from the efficient conduct of School business, or involves accessing or sending unlawful, offensive or inappropriate material (for example, obscene, discriminatory or abusive material), is prohibited; and, consequently, monitoring may take place to detect or investigate such behaviour.

Monitoring for operational reasons

Most ICT systems within the School are monitored to ensure that they are performing properly. This reflects standard good practice, and normally involves only anonymous aggregate data that does not identify individuals or the contents of their communications.

However, a general exemption in the *Regulation of Investigatory Powers Act 2000 (as amended)* permits the School to intercept certain communications where the interception is by an authorised person for purposes connected with the provision or operation of a service. For example, the School may:

- Examine misaddressed messages in order to redirect them as necessary, or check email subject lines for malicious code;
- Monitor system traffic to determine its source, where this is necessary to ensure the effective performance of their mail servers; for example, to eliminate unsolicited commercial email; and
- Investigate which system and/or individual is the source of a denial of service attack.

ii. Authorisation of monitoring of computer or network use

Routine monitoring for operational reasons and monitoring, or access to stored material to investigate policy (or legal) compliance matters, may be authorised by the Headmaster.

iii. Access to stored documents (including email) for business purposes

There are occasions when the School needs to access information held by a user of the School's systems either within an email, on their computer or other files stored or backed up. This might occur, for example, when an employee is absent, either through illness or on leave, and a situation arises which requires a rapid response. Staff and pupils must be made aware that the School reserves the right to obtain access to files held on or in equipment owned by the School, and that the privacy of personal material stored on or in such equipment in the event of authorised access cannot be guaranteed.

iv. Exceptional modification of user files

In exceptional circumstances, system custodians may need to make changes to user filestore. Examples include disabling programs which may adversely affect system or network performance, disabling software which is being used contrary to licensing arrangements or removing from public view confidential files or offensive material.

The permission of the file owner should be obtained unless the situation is of such urgency as to make this impracticable. The associated justification for this decision must be logged. The file owner must be informed of the change and the justification.

The system custodian may not, without specific authorisation from the appropriate authority, modify the contents of any file in such a way as to damage or destroy information. If necessary, files should be moved to a secure off-line archive.

v. Web filtering and monitoring

Web filtering systems are in place to restrict access to potentially harmful or inappropriate websites and to reduce the risks posed by such sites both to the welfare of pupils and to the security of the IT network. Web filtering applies to both the School site (hardware located and used on the premises) and to School issued devices beyond the premises connected to the School's network.

Web filtering mitigates the risk of School ICT being used for unlawful activity, whilst supporting pupils and staff to remain on task. Examples of content and sites web filtering is designed to block include pornography, violence and extremism, and gambling.

Web filtering produces reports of activity flagged for concern, based upon highly developed specialist algorithms. Should activity, such as a search term or website entry, meet a higher threshold for concern it is reported in real time to senior staff responsible for safeguarding. This allows for the circumstances to be quickly considered and investigated, helping identify any safeguarding or child protection risks. It is recognised that innocent behaviour, such as a search for content within an appropriate business/educational context, can sometimes trigger the web filtering system and that there will therefore not always be cause for concern.

Web filtering and monitoring does not seek to prevent reasonable personal use under the terms of this policy and resultant data will only be utilised in a way relevant to the aims of monitoring set out in this Policy.

LINKED POLICIES	❑ Governors' Statement of Education ❑ School Priorities for Development ❑ Bullying Policy ❑ Code of Conduct for Staff and Governors ❑ Complaints Policy ❑ Data Protection Policy ❑ Equal Opportunities Policy ❑ Health and Safety Policy ❑ Home-School Agreement ❑ Pupil Discipline Policy ❑ Safeguarding Policy ❑ Staff Disciplinary Procedure ❑ Staff Grievance Procedure ❑ Whistleblowing Policy

LINKED LEGISLATION AND REFERENCE MATERIALS

- ❑ Data Protection Act 2018
- ❑ UK General Data Protection Regulation
- ❑ Computer Misuse Act 1990
- ❑ Copyright, Designs and Patents Act 1988 (as amended)
- ❑ Regulation of Investigatory Powers Act 2000 (as amended)
- ❑ Data Retention and Investigatory Powers Act 2014
- ❑ Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- ❑ Equality Act 2010
- ❑ Part-Time Workers (Prevention of Less Favourable Treatment) Regulations 2000
- ❑ Fixed-Term Employees (Prevention of Less Favourable Treatment) Regulations 2002
- ❑ Obscene Publications Act 1959 (as amended)
- ❑ Race Relations Act 1976 (as amended)
- ❑ Protection from Harassment Act 1997
- ❑ Protection of Children Act 1978 (as amended)
- ❑ Public Order Act 1986 (as amended)
- ❑ Criminal Justice and Public Order Act 1994 (as amended)
- ❑ Terrorism Act 2006
- ❑ Terrorism Prevention and Investigation Measures Act 2011
- ❑ Counter-Terrorism and Security Act 2015
- ❑ Human Rights Act 1998
- ❑ *CHEST Code Of Conduct For The Use Of Software Or Datasets* http://www.eduserv.org.uk/services/Chest-Agreements/about-chest
- ❑ JISC Model Licences http://www.jisc.ac.uk/publications/programmerelated/2009/scaiprtoolkit/2modellicence.aspx
- ❑ The Employment Practices Data Protection Code Part 3 Monitoring at work https://www.igt.hscic.gov.uk/KnowledgeBaseNew/ICO%20Employment%20Practices%20Code_Part3Monitoring%20at%20Work.pdf

Approved by the Governing Body on 2 November 2023

Signed ....

A.N. Gaskell, Chairman of the Governing Body