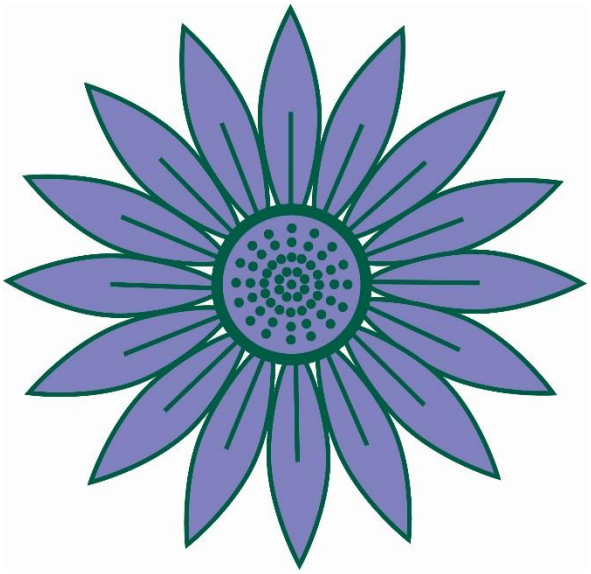

MAYFIELD GRAMMAR SCHOOL

GRAVESEND

IT ACCEPTABLE USE POLICY

For Students and Parents

Mayfield Grammar School, Gravesend

IT ACCEPTABLE USE POLICY

1. Introduction and aims

ICT is an integral part of the way our school operates, and is a critical resource for pupils, staff, governors, volunteers and visitors. It supports teaching and learning, pastoral and administrative functions of the school.

However, the ICT resources and facilities also pose risks to data protection, online safety and safeguarding.

This policy aims to:

- Set guidelines and rules on the use of school ICT resources for staff, pupils, parents and governors
- Establish clear expectations for the way all members of the school community engage with each other online
- Support the school's policy on data protection, online safety and safeguarding
- Prevent disruption to the school through the misuse, or attempted misuse, of ICT systems
- Support the school in teaching pupils safe and effective internet and ICT use
- Support the pupils to become empowered and responsible digital creators and users

This policy covers all users of our school's ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors.

Breaches of this policy may be dealt with under our Staff Code of Conduct.

2. Relevant legislation and guidance

This policy refers to, and complies with, the following legislation and guidance:

- Data Protection Act 2018
- The General Data Protection Regulation
- Computer Misuse Act 1990
- Human Rights Act 1998
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Education Act 2011
- Freedom of Information Act 2000
- The Education and Inspections Act 2006
- Keeping Children Safe in Education 2019
- Searching, screening and confiscation: advice for schools

3. Definitions

- **"ICT facilities":** includes all facilities, systems and services including but not limited to network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service which may become available in the future which is provided as part of the ICT service
- **"Users":** anyone authorised by the school to use the ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors
- **"Personal use":** any use or activity not directly related to the users' employment, study or purpose
- **"Authorised personnel":** employees authorised by the school to perform systems administration and/or monitoring of the ICT facilities
- **"Materials":** files and data created using the ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites, and blogs

4. Unacceptable use

The following is considered unacceptable use of the school's ICT facilities by any member of the school community. Any breach of this policy may result in disciplinary or behaviour proceedings (see section 4.2 below).

Unacceptable use of the school's ICT facilities includes:

- Using the school's ICT facilities to breach intellectual property rights or copyright
- Using the school's ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- Activity which defames or disparages the school, or risks bringing the school into disrepute. We encourage all students and staff to check any correspondence with a member of SLT to ensure it is appropriate for distribution.
- Sharing confidential information about the school, its pupils, or other members of the school community
- Connecting any device to the school's ICT network without approval from authorised personnel
- Setting up any software, applications or web services on the school's network without approval by authorised personnel, or creating or using any program, tool or item of software designed to interfere with the functioning of the ICT facilities, accounts or data
- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- Causing intentional damage to ICT facilities
- Removing, deleting or disposing of ICT equipment, systems, programs or information without permission by authorised personnel

- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
- Using inappropriate or offensive language
- Promoting a private business, unless that business is directly related to the school
- Using websites or mechanisms to bypass the school's filtering mechanisms

This is not an exhaustive list. The school reserves the right to amend this list at any time. The Headteacher will use professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the school's ICT facilities, or its use is in breach of the school behaviour policy or school Code of Conduct.

4.1 Exceptions from unacceptable use

Where the use of school ICT facilities is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the Headteacher's discretion.

Please submit your request in writing to the Assistant Headteacher responsible for IT, who will deal with this appropriately. Please allow up to 2 weeks for this matter to be dealt with. If this request involves data sharing with a third party, you will be required to complete a Privacy Impact Assessment and await all necessary confirmation before proceeding.

4.2 Sanctions

Pupils and staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with the school's behaviour policy or the school Code of Conduct

Students may find their ICT privileges indefinitely revoked for any inappropriate ICT conduct.

The School Behaviour Policy can be found on the School website by clicking on the 'About Mayfield' tab and clicking 'Policies'.

5. Pupils

5.1 Access to ICT facilities

All students must abide by the strict conditions for computer usage outside of lesson time. The following information is provided as guidance for this use:

- Sixth Form students are permitted to independently access the computers in the Sixth Form Study area and tablets in the school canteen during their Study Periods. This usage is monitored by the Network Manager using Impero and should only be for education purposes.
- All other students must use computers in the LRC and tablets in the school canteen during break and lunch times where adult supervision is provided. These must also be used for education purposes only.
- Specialist ICT equipment, such as that used for music or design and technology must only be used under the supervision of staff.

5.1.1 Use of phones and email

The school provides each student with an email address.

This email account should be used for school work purposes only and not for general correspondence. All correspondence issued to other students and/or staff must be checked by a member of the Senior Leadership Team before sending.

All work-related business should be conducted using the email address the school has provided.

Students must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract. In order to ensure that correspondence is appropriate for distribution, all staff must check with their line manager before sending.

If students receive an email in error, the sender should be informed and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.

If students send an email in error which contains the personal information of another person, they must inform the School's Network Manager (Mr Wicks) immediately and follow our data breach procedure.

5.2 Search and deletion

Under the Education Act 2011, and in line with the Department for Education's guidance on searching, screening and confiscation, the school has the right to ask pupils to show DSL's that any pornographic images or any other data or items banned under school rules or legislation are deleted from pupils' phones, computers or other devices. Parents will also be contacted, who will be asked to check the device at home too.

The school can, and will, delete files and data found on monitored devices within the school network if we believe the data or file has been, or could be, used to disrupt teaching or break the school's rules.

5.3 Remote access

The school allows students to access the school's ICT facilities and materials remotely.

The remote access system allows all students to access their user area from outside the school site. Instructions for how to remotely access your school user area can be found at vle.mgsg.kent.sch.uk by clicking the Remote Access icon.

Students accessing the school's ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on-site. They must be particularly vigilant if they use the school's ICT facilities outside the school and take such precautions as the Network Manager may require from time to time against importing viruses or compromising system security.

Our ICT facilities contain information which is confidential and/or subject to data protection legislation. Students are only provided access to their user area and the students 'Shared Documents' folder.

The school's Data Protection Policy can be found on the school's website by clicking on 'About Mayfield' and then 'Policies'.

5.4 Unacceptable use of ICT and the internet outside of school

The school will sanction pupils, in line with the behaviour policy if a pupil engages in any of the following **at any time** (even if they are not on school premises):

- Using ICT or the internet to breach intellectual property rights or copyright
- Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures

- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, other pupils, or other members of the school community
- Gaining or attempting to gain access to restricted areas of the network, or to any password protected information, without approval from authorised personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- Causing intentional damage to ICT facilities or materials
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
- Using inappropriate or offensive language

6. Parents

6.1 Access to ICT facilities and materials

Parents do not have access to the school's ICT facilities as a matter of course.

However, parents working for, or with, the school in an official capacity (for instance, as a volunteer or as a member of the PTA) may be granted an appropriate level of access, or be permitted to use the school's facilities at the headteacher's discretion.

Where parents are granted access in this way, they must abide by this policy as it applies to all staff.

6.2 Communicating with or about the school online

We believe it is important to model for pupils, and help them learn, how to communicate respectfully with, and about, others online.

Parents play a vital role in helping model this behaviour for their children, especially when communicating with the school through our website and social media channels.

We ask parents to sign the agreement in appendix 2.

7. Data security

The school takes steps to protect the security of its computing resources, data and user accounts. However, the school cannot guarantee security. Staff, pupils, parents and others who use the school's ICT facilities should use safe computing practices at all times.

7.1 Passwords

All users of the school's ICT facilities should set strong passwords for their accounts and keep these passwords secure.

Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control.

Members of staff or pupils who disclose account or password information may face disciplinary action. Parents or volunteers who disclose account or password information may have their access rights revoked.

Upon entry into Year 7, students are provided with a standard school password for first user access. Upon signing onto the network for the first time, they are then prompted to set their own password. Students are able to change this password at any time.

7.2 Software updates, firewalls, and anti-virus software

All of the school's ICT devices that support software updates, security updates, and anti-virus products will be configured to perform such updates regularly or automatically.

Users must not circumvent or make any attempt to circumvent the administrative, physical and technical safeguards we implement and maintain to protect personal data and the school's ICT facilities.

Any personal devices using the school's network must all be configured in this way.

7.3 Data protection

All personal data must be processed and stored in line with data protection regulations and the school's data protection policy. This can be found on the school website by clicking 'About Mayfield' and then 'Policies'.

7.4 Access to facilities and materials

All users of the school's ICT facilities will have clearly defined access rights to school systems, files and devices.

These access rights are managed by the School's Network Manager.

Users should not access, or attempt to access, systems, files or devices to which they have not been granted access. If access is provided in error, or if something a user should not have access to be shared with them, they should alert the School's Network Manager immediately.

Users should always log out of systems and lock their equipment when they are not in use to avoid any unauthorised access. Equipment and systems should always be logged out of and closed down completely at the end of each working day.

7.5 Encryption

The school ensures that its devices and systems have an appropriate level of encryption.

School staff may only use personal devices (including computers and USB drives) to access school data, work remotely, or take personal data (such as pupil information) out of school if they have been specifically authorised to do so by the Headteacher.

Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption, as defined by the Network Manager.

8. Internet access

The school's wireless internet connection is secured and filtered using 'Smoothwall'. The school's filtering system is owned by Cantium, but slight amendments may be requested by the School Network Manager. The School Network Manager will test the filtering system once per term, to ensure the network is filtering correctly.

All staff have staff access to the school's computer system, which allows web access to sites such as YouTube for teaching purposes. Staff also have access to the staff shared area and student shared area on the school network.

All Lower School and Upper School students have student privileges that do not permit the use of websites such as YouTube etc. and also only allow access to the student shared area on the school network. Sixth Form students are able to view websites for learning purposes such as Youtube etc.

8.1 Pupils

Sixth Form pupils may access the MGSG BYOD wi-fi when bringing their own device into school. All devices on this wi-fi will comply with the school's filtering system with the school's internal servers being protected from any external threats. If students have any questions regarding the use of MGSG BYOD, they must direct them to the school's Network Manager.

8.2 Visitors

Any visitor to the school may request access to the school wi-fi network. However, this will only be permitted by the school's Network Manager and any use of the school's wi-fi network by a visitor will be monitored by internal systems.

9. Monitoring and review

The Headteacher and Network Manager monitor the implementation of this policy, including ensuring that it is updated to reflect the needs and circumstances of the school.

This policy will be reviewed 2 years and presented to the school's governing board in September of each review period.

The governing board is responsible for approving this policy.

10. Related policies and documents

This policy should be read alongside the school's policies on:

- Online Safety Policy
- Safeguarding and Child Protection Policy
- Behaviour Policy
- Staff Code of Conduct
- Data Protection Policy

Appendix 1: Acceptable use of the Internet: agreement for parents and carers

Acceptable use of the Internet: agreement for parents and carers	
Name of parent/carer: **Name of child:**	
• I have read and discussed the IT Acceptable Use Policy with my child. • I know my child will receive online safety education to help them understand the importance of safe use. • I understand that if the school has any concerns regarding my child's safety online, whether in school or at home, I will be contacted immediately. • I will contact the school's online safety coordinator if I have any concerns regarding online safety. • I will visit the National Online Safety website if I require additional information regarding the applications my child uses.	
Online channels are an important way for parents/carers to communicate with, or about, our school. I accept that the school uses the following channels: • Our official Twitter accounts. • Email/text groups for parents (for school announcements and information). I accept that some parents/carers also set up independent channels to help them stay on top of what's happening in their child's class. For example, class/year Facebook groups, email groups, or chats (through apps such as WhatsApp).	
When communicating with the school via official communication channels, or using private/independent channels to talk about the school, I will: • Be respectful towards members of staff, and the school, at all times. • Be respectful of other parents/carers and children. • Always direct any complaints or concerns through the school's official channels, so they can be dealt with in line with the school's complaints procedure. • Accept that staff may not be able to respond to my complaints or concerns on the day they are received, but will make contact within 48 hours. • Respect the rights of other members of the school community by uploading or sharing photos or videos on social media of any child other than my own, unless I have the permission of other children's parents/carers.	
Signed:	**Date:**

Appendix 2: Acceptable use agreement for pupils

Acceptable use of the school's ICT facilities and internet: agreement for pupils	
Name of pupil:	
When using the school's ICT facilities and accessing the internet (including MGSG BYOD and cellular connections) in school, I will: • Use them only for educational purpose. • Use them only with a teacher being present, or with a teacher's permission. • Use them in accordance with the School's Code of Conduct. • Access only appropriate websites that remain unblocked. • Access social networking sites only when my teacher has expressly allowed this as part of a learning activity. • Open any attachments in emails, or follow any links in emails, only by first checking with a teacher. • Formally communicate via email, starting this with 'Dear ……'. • Use only appropriate language when communicating online. • Keep my password secure and only login to my school account. • Uphold Mayfield's Expectations. I understand that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. I will immediately inform a teacher or other member of staff if I find any material which might upset, distress or harm me or others. I will always use the school's ICT systems and internet responsibly. I understand that the school can issue sanctions if I do not behave appropriately online, even if I'm not in school when I do them.	
Signed (pupil):	**Date:**
Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 3: IT Acceptable Use Agreement: BYOD Permission (Sixth Form Only)

Acceptable use of the school's BYOD Wi-Fi system

Name of pupil/staff member/governor/volunteer/visitor:

The school provides Wi-Fi for the school community and allows access for educational purposes only.

- The use of ICT devices falls under Mayfield Grammar School's IT Acceptable Use Policy, Online Safety Policy and Behaviour Policy which all students, staff, governors, visitors and volunteers must agree to and comply with.
- The school reserves the right to limit the bandwidth of the wireless service, as necessary, to ensure network reliability and sharing of network resources for all users.
- School owned information systems, including Wi-Fi, must be used lawfully and I understand the Computer Misuse Act 1990 makes the following criminal offences to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.
- I will take all practical steps necessary to make sure that any equipment connected to the schools service is adequately secure (such as up-to-date anti-virus software and systems updates).
- The school's wireless service is not secure, and the school cannot guarantee the safety of traffic across it. Use of the school's wireless service is done at my own risk. By using this service, I acknowledge that security errors and hacking are an inherent risk associated with any wireless network. For that reason, I expressly agree that I knowingly assume such risk, and further agree to hold the school harmless from any claim or loss arising out of, or related to, any such instance of hacking or other authorised use or access into my computer device.
- The school accepts no responsibility for any software downloaded and/or installed, e-mails opened, or sites accessed via the school's wireless service connection to the Internet. Any damage done to equipment for any reason including, but not limited to, viruses, identity theft, spyware, plug-ins or other Internet-borne programs is my sole responsibility; and I indemnify and hold harmless the school from any such damage.
- The school accepts no responsibility regarding the ability of equipment, owned by myself, to connect to the school's wireless service.
- I will respect system security and I will not disclose any password or security information that is given to me. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate.
- I will not attempt to bypass any of the school's security and filtering systems or download any unauthorised software of applications.
- My use of the school Wi-Fi will be safe and responsible and will always be in accordance with the school IT AUP and the Law including copyright and intellectual property rights. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites.
- I will not upload, download, access or forward any material which is illegal or inappropriate or cause any harm, distress or offence to any other person, or anything which could bring the school into disrepute.
- I will report any online safety concerns, filtering breaches or receipt of inappropriate materials to the Assistant Headteacher responsible for IT and/or the School Network Manager.
- If I have any queries or questions regarding safe behaviour online, then I will discuss this with my Digital Leader or the Assistant Headteacher responsible for IT.

I understand that my use of the schools Wi-Fi network will be monitored and recorded to ensure policy compliance in accordance with privacy and data protection legislation. If the school suspects that unauthorised and/or inappropriate behaviour may be taking place, then the school may terminate or restrict further usage. If the School suspects that the system may be being used for criminal purposes then the matter will be brought to the attention of the relevant law enforcement organisation.	
Signed (pupil/staff member/governor/volunteer/visitor):	**Date:**