WOLVERHAMPTON GRAMMAR SCHOOL
IT ACCEPTABLE USE POLICY FOR PUPILS

1 Scope

1.1 This policy is addressed to all pupils, and parents are encouraged to read it with their child. A copy of the policy is available on the School website, and the School actively promotes the participation of parents to help the School safeguard the welfare of pupils and promote the safe use of technology by provision of both electronic information and through Pastoral Parents' Evenings.

1.2 The School will take a wide and purposive approach to considering what falls within the meaning of technology. This policy relates to all technology, computing and communications devices, network hardware and software, and services and applications associated with them including:

- the internet
- email
- mobile phones and smartphones
- desktops, laptops, netbooks, tablets / phablets
- personal music players
- devices with the capability for recording and / or storing still or moving images
- social networking, micro blogging and other interactive web sites
- instant messaging (including image and video messaging via apps such as Snapchat and WhatsApp), chat rooms, blogs and message boards
- webcams, video hosting sites (such as YouTube)
- gaming sites
- Firefly, the School's Virtual Learning Environment
- SMART boards
- other photographic or electronic equipment e.g. GoPro devices.

1.3 This policy applies to the use of technology on School premises.

1.4 This policy also applies to the use of technology off School premises if the use involves pupils or any member of the School community or where the culture or reputation of the School are put at risk.

2 Aims

2.1 The aims of this policy are:

- to educate and encourage pupils to make good use of the educational opportunities presented by access to technology;
- to safeguard and promote the welfare of pupils, in particular by anticipating and preventing the risks arising from:
    - exposure to harmful or inappropriate material (such as pornographic, racist, extremist or offensive materials);

- the sharing of personal data, including images;
- inappropriate online contact or conduct; and
- cyberbullying and other forms of abuse;

- to minimise the risk of harm to the assets and reputation of the School;
- to help pupils take responsibility for their own safe use of technology (i.e. limiting the risks that children and young people are exposed to when using technology);
- to ensure that pupils use technology safely and securely and are aware of both external and peer to peer risks when using technology;
- to prevent the unnecessary criminalisation of pupils;
- to clarify the expectations of pupils when using School equipment or when bringing devices into School.

3 Safe use of technology

3.1 We want pupils to enjoy using technology and to become skilled users of online resources and media. We recognise that this is crucial for further education and careers.

3.2 The School will support pupils to develop their skills and make internet access as unrestricted as possible whilst balancing the safety and welfare of pupils and the security of systems. Pupils are educated about the importance of safe and responsible use of technology to help them to protect themselves and others online.

3.3 The School provides a filtered internet service to help protect pupils in keeping themselves safe on line. However, no system can be completely effective and the School cannot accept liability for materials accessed by pupils, or any consequences thereof.

3.4 Pupils may find the following resources helpful in keeping themselves safe online:

- http://www.thinkuknow.co.uk/
- http://www.childnet.com/young-people
- https://www.saferinternet.org.uk/advice-centre/young-people
- https://www.disrespectnobody.co.uk/
- http://www.safetynetkids.org.uk/
- http://www.childline.org.uk/Pages/Home.aspx

3.5 Please see the School's safeguarding policy and anti-bullying policy for further information about the School's online safety strategy.

3.6 Please see any member of the School's safeguarding team if you have any queries or concerns.

4 Internet and email

4.1 The School provides internet access and an email system to pupils to support their academic progress and development.

4.2 All pupils will receive guidance on the use of the School's internet and email systems. If a pupil is unsure about whether they are doing the right thing, they must seek assistance from a member of staff.

4.3 For the protection of all pupils, their use of email and of the internet will be monitored by the School. Pupils should remember that even when an email, data or files that have been downloaded has been deleted, it can still be traced on the system. Pupils should not assume that files stored on servers or storage media are always private.

5 ICT rules

5.1 Pupils **must** comply with the following rules and principles:

- access and security (Appendix 1);
- use of internet and email (Appendix 2);
- use of mobile electronic devices (Appendix 3); and
- photographs and images (including "sexting") (Appendix 4).

5.2 The purpose of these rules is to set out the principles which pupils must bear in mind at all times and also the rules which pupils must follow to use technology safely and securely.

5.3 These principles and rules apply to all use of technology.

6 Procedures

6.1 Pupils are responsible for their actions, conduct and behaviour when using technology. Use of technology should be safe, responsible, respectful to others and legal. If a pupil is aware of misuse by other pupils, they should talk to a teacher about it as soon as possible.

6.2 Any misuse of technology by pupils will be dealt with under the School's behaviour management policy.

6.3 Pupils must not use their own or the School's technology to bully others. Bullying incidents involving the use of technology will be dealt with under the School's anti-bullying policy. If a pupil thinks that they might have been bullied or that another person is being bullied, they should talk to a teacher about it as soon as possible. See the School's anti-bullying policy for further information about cyberbullying and e-safety, including useful resources.

6.4 In any cases giving rise to safeguarding concerns, the matter will be dealt with under the School's child protection procedures (see the School's safeguarding policy). If a pupil is worried about something that they have seen on the internet, or on any electronic device, including on another person's electronic device, they must tell a teacher about it as soon as possible.

6.5 In a case where the pupil is considered to be vulnerable to radicalisation they may be referred to a member of staff immediately. Channel is a programme which focuses on support at an early stage to people who are identified as being vulnerable to being drawn into terrorism.

6.6 In addition to following the procedures in the relevant policies as set out above, all serious incidents involving technology must be reported to a Designated Safeguarding Lead and the Systems Director who will record the matter centrally in the Technology Incidents Log.

7 Sanctions

7.1 Where a pupil breaches any of the School rules, practices or procedures set out in this policy or the appendices, the Governors have authorised the Head to apply any sanction which is appropriate and proportionate to the breach in accordance with the School's behaviour management policy including, in the most serious cases, exclusion. Other sanctions might include: increased monitoring procedures, withdrawal of the right to access the School's internet and email facilities and detention. Any action taken will depend on the seriousness of the offence.

7.2 Unacceptable use of electronic devices or the discovery of inappropriate data or files could lead to confiscation of the device or deletion of the material in accordance with the practices and procedures in this policy and the School's behaviour management policy. Students found in possession of a mobile phone or device during a public examination will be reported to the appropriate examining body. This may result in that student's withdrawal from either that examination or all examinations.

7.3 The School reserves the right to charge a pupil or their parents for any costs incurred to the School as a result of a breach of this policy.

8 Monitoring and review

8.1 All serious incidents involving the use of technology will be logged centrally in the Technology Incident Log by the Designated Safeguarding Lead and the Systems Director.

8.2 The Systems Director and the team of Designated Safeguarding Leads have responsibility for the implementation and review of this policy:

- the Systems Director is responsible for the effective operation of the School's network. They monitor the use of technology as set out in this policy and maintain the appropriate logs and will review the policy on a regular basis to ensure that it remains up to date with technological changes;
- the team of Designated Safeguarding Leads will consider the record of technology safety incidents and the logs of internet activity (including sites visited) as part of the ongoing monitoring of safeguarding procedures, to consider whether existing security and safety practices within the School are adequate.

8.3 Consideration of the efficiency of the School's e-safety procedures and the education of pupils about keeping safe online will be included in the Governors' annual review of safeguarding.

Please also refer to the following policies:

Behaviour Management Policy - website	Safeguarding Policy - website
Anti-Bullying Policy - website	Privacy Notice for Pupils and Parents - website

Taking, Storing and Using Images of Children Policy – website.	CCTV Policy - website

Monitoring and Evaluation of this policy

The School monitors and evaluates its IT Acceptable Use Policy for Pupils through the following activities:

- Annual Governing body safeguarding review.
- Senior leadership team and safeguarding team discussion
- Regular analysis of a range of risk assessments
- Annual Student Bullying Survey
- Feedback from Peer Support and Student Parliament
- Logs of bullying/racist behaviour/complaints are reviewed annually by the senior leadership team and the governing body
- Scrutiny of complaints and concerns by SMT and Board of Directors.

NJCA
September 2018

Next Review:
September 2019

Appendix 1 Access and security

1 Access to the internet from the School's computers and network must be for educational purposes only. You must not use the School's facilities or network for personal, social or non-educational use.

2 You must not knowingly obtain (or attempt to obtain) unauthorised access to any part of the School's or any other computer system, or any information contained on such a system.

3 No laptop or other mobile electronic device may be connected to the School network without the consent of the IT department unless this device is part of the mobile device enrolment program.

4 You are advised not to use cellular data (e.g. GPRS, 3G, 4G, third party Wi-Fi Services) to access the internet while you are on School premises, as you would not benefit from the School's filtering and anti-virus software.

5 Passwords protect the School's network and computer system. You must not let anyone else know your password. If you believe that someone knows your password, you must change it immediately. Passwords must be secure with a minimum of 8 characters including a mixture of numbers and symbols.

6 You must not attempt to gain unauthorised access to anyone else's computer or mobile device or to confidential information to which you are not authorised to access. If there is a problem with your passwords, you should speak to your class teacher or contact ICT Support.

7 You must not attempt to access or share information about others. To do so may breach data protection legislation and laws relating to confidentiality.

8 The School has a firewall in place to ensure the safety and security of the School's networks. You must not attempt to disable, defeat or circumvent any of the School's security facilities. Any problems with the firewall must be reported to the class teacher or ICT Support.

9 The School has filtering systems in place to block access to unsuitable material, wherever possible, to protect the welfare and safety of pupils. You must not try to bypass this filter. If you require content that has been filtered, then you may submit a request via a form in Firefly to your Head of Year. The use of VPN's is strictly forbidden.

10 Viruses can cause serious harm to the security of the School's network and that of others. Viruses are often spread through internet downloads or circulated as attachments to emails. If you think or suspect that an attachment, or other downloadable material, might contain a virus, you must speak to ICT Support before opening the attachment or downloading the material.

11 You must not disable or uninstall any anti-virus software on the School's computers.

12 The use of location services represents a risk to the personal safety of those within the School community, the School's security and its reputation. You should always consider whether it is appropriate to use location services on any website or application, whether on a School or personal device, with the capability of identifying the user's location while on School premises or otherwise in the course of School related activities.

13 If you are the victim of a cybercrime or on-line fraud, or attempted cybercrime or on-line fraud, you must inform the Network Manager immediately. This is to ensure the integrity of the School system is not compromised.

Appendix 2 Use of the internet and email

1 The School does not undertake to provide continuous internet access. Email and website addresses at the School may change from time to time.

Use of the internet

2 You must use the School's computer system for educational purposes only. The School has filtering systems in place to block access to unsuitable material, wherever possible, to protect the welfare and safety of pupils. You must not try to bypass this filter. If you require content that has been filtered, then you may submit a request via a form in Firefly to your Head of Year. The use of VPN's is strictly forbidden.

3 You must take care to protect personal and confidential information about yourself and others when using the internet, even if information is obtained inadvertently. You should not put personal information about yourself, for example your full name, address, date of birth or mobile number, online.

4 You must not load material from any external storage device brought in from outside the School onto the School's systems, unless this has been authorised by ICT Support. The schools learning platform and Foldr applications provide 24/7 access to material and home folder content.

5 You should assume that all material on the internet is protected by copyright and such material must be treated appropriately and in accordance with the owner's rights - you must not copy (plagiarise) another's work.

6 You must not view, retrieve, download or share any offensive material. Offensive material includes, but is not limited to, content that is abusive, racist, considered to be of an extreme or terrorist related nature, sexist, homophobic, any form of bullying, pornographic, defamatory or criminal activity. Use of technology in this way is a serious breach of discipline and may constitute a serious criminal offence. You must tell a member of staff immediately if you have accidentally read, downloaded or have been sent any offensive material or material that is inappropriate, including personal information about someone else.

7 You must not communicate with staff using social networking sites or other internet or web-based communication channels unless this is expressly permitted for educational reasons.

8 You must not bring the School into disrepute through your use of the internet.

Use of email

9 You must not use any personal web-based email accounts such as Gmail, Yahoo or Hotmail through the School's network. This will be unnecessary as you are provided with your own email account for School purposes.

10 Your School email accounts can be accessed from home by the link in Firefly.

11 You must use your School email accounts for any email communication with staff. Communication either from a personal email account or to a member of staff's personal email account is not permitted.

12 Email should be treated in the same way as any other form of written communication. You should not include or ask to receive anything in an email which is not appropriate to be published generally or which you believe the School and / or your parents would consider to be inappropriate. Remember that emails could be forwarded to or seen by someone you did not intend.

13 You must not send or search for any email message which contains offensive material. Offensive material includes, but is not limited to, content that is abusive, racist, considered to be of an extreme or terrorist related nature, sexist, homophobic, any form of bullying, pornographic, defamatory or criminal activity. If you are unsure about the content of a message, you must speak to a member of staff. If you come across such material, you must inform a member of staff as soon as possible. Use of the email system in this way is a serious breach of discipline and may constitute a criminal offence.

14 Trivial messages and jokes should not be sent or forwarded through the School's email system. Not only could these cause distress to recipients (if considered to be inappropriate) but also creates unnecessary system traffic and storage.

15 You must not read anyone else's emails without their consent.

Appendix 3 Mobile Phones and Devices Guidelines (Pupils)

Principle

1 We believe there are tangible educational benefits to allowing mobile device use at WGS and as such pupils are encouraged to bring phones/mobile devices into School.

2 Pupils are responsible for the mobile phones and devices they bring to School. WGS accepts no responsibility for their loss, theft or damage.

3 All use of mobile devices at School is open to scrutiny. The Head may withdraw or restrict authorisation for use at any time if it is deemed necessary.

General use around WGS

4 Pupils must be clear about when it is appropriate to use phones and mobile devices. What follows is a list of times when it is appropriate, and when it is not. The list is not definitive: judgment must be used.

5 It is appropriate to use phones and devices at School

- during lessons and formal School time as part of an approved and directed curriculum-based activity with consent from an appropriate member of staff. Recording, taking and sharing of images, video and audio on any mobile device must be explicitly agreed by the teacher.
- in the library to assist with academic work.
- before School, at break, at lunch and after School, so long as it does not conflict with any other obligations you may have.

6 It is not appropriate to use phones and devices at School

- walking between lessons: doing so might make you late, and it may be hazardous.
- in areas where pupils are most vulnerable, such as toilets and changing areas.
- in tutor times and lunch in The Derry. At such time it is more important to talk to people face to face.

7 At times when it is not appropriate to use phones or mobile devices they should be kept on silent and not on vibrate. You should not be in a position to be distracted by them.

8 Pupils are required to own and use a suitable pair of earphones for use with their mobile electronic device.

Examinations

9 In examinations, mobile devices are banned because they are potentially a means to cheat. It is for this reason that:

- Phones and devices must not be taken into external examinations, controlled assessments, oral exams etc. Pupils found in possession of a mobile phone during a

public examination will be reported to the appropriate examining body. This may result in that pupil's withdrawal from either that examination or all examinations.

- For internal exams, phones and devices must be switched off and not used in any way. They must not be on your person.

Misuse

10 Messaging on devices should always be respectful: pupils must take every care to ensure they are not, or cannot be suspected of being a cyber-bully. It is therefore important that the recording, taking and sharing of images, video and/or audio on any mobile device, must be explicitly agreed by the person (whether teacher or pupil) being recorded.

11 The School reserves the right to search the content of any mobile or handheld device on WGS premises where there is a reasonable suspicion that it may contain undesirable material, including promotion of pornography, violence or bullying.

12 If a pupil breaches the School guidelines then the phone or device may be confiscated. In such a circumstance it will be held in a secure place for the duration of the lesson during which the breach occurred, or in more serious instances, passed on to more senior staff.

Contact with staff

13 Pupils must not use mobile phones or devices for contacting staff other than via School email or the schools Firefly learning platform.

Appendix 4 Photographs and images

1 Using photographic material of any kind to bully, harass or intimidate others will not be tolerated and will constitute a serious breach of discipline.

2 You may only use cameras or any mobile electronic device to take a still or moving image with the express permission of the member of staff in charge and with the permission of those pupils or staff appearing in the image.

3 You must allow staff access to images stored on mobile phones and / or cameras and must delete images if requested to do so.

4 The posting of images which in the reasonable opinion of the School is considered to be offensive or which brings the School into disrepute on any form of social media or websites such as YouTube etc is a serious breach of discipline and will be subject to disciplinary procedures whatever the source of the material, irrespective of whether the image was posted using School or personal facilities.

Sexting

5 "Sexting" means the taking and sending or posting of images or videos of a sexual or indecent nature of you or another young person, usually through mobile picture messages or webcams over the internet.

6 Sexting is strictly prohibited, whether or not you are in the care of the School at the time the image is recorded and / or shared.

7 Sexting may be a criminal offence, even if the picture is taken and shared with the permission of the person in the image. Even if you are not prosecuted, this may result in information being stored on your police record, which may prevent you from undertaking certain jobs in the future.

8 The police may seize any devices which they believe may have been used for sexting. If the police find that a device contains inappropriate images, they are unlikely to return it to you.

9 Remember that once a photo or message is sent, you have no control about how it is passed on. You may delete the image but it could have been saved or copied and may be shared by others.

10 Images shared online become public and may never be completely removed. They could be found in the future by anyone, even by universities and future employers.

11 Do not take or store indecent images of yourself. Even if you don't share them yourself, there is a risk that you may lose your device, it may be "hacked", or its data may still be accessible to a future owner.

12 The School will treat incidences of sexting (both sending and receiving) as a breach of discipline and also as a safeguarding matter under the School's child protection procedures (see the School's safeguarding policy and procedures).

13 If you are concerned about any image you have received, sent or forwarded or otherwise seen, speak to any member of staff for advice.