Acceptable Use of Technology Policy for Pupils

Stockport Grammar School

April 2019

Contents

1 Aims 3
2 Scope and application 3
3 Regulatory framework 3
4 Publication and availability 4
5 Definitions 4
6 Responsibility statement and allocation of tasks 4
7 Safe use of technology 4
8 Internet and email 5
9 School rules 5
10 Procedures 6
11 Sanctions 6
12 Training 7
13 Risk assessment 7
14 Record keeping 7
15 Version control 7

Sections

Section 1 Access and security 8
Section 2 Use of the internet and email 9
Section 3 Use of mobile electronic devices 10
Section 4 Photographs and images 11

Appendix 1 The Legal Stuff 13

Appendix 2 Acceptable Use Agreement

1 Aims

Access to technology is now an integral part of daily life; however it's important to be able to use it safely and whilst this policy may seem very formal it sets out how the School believes you should make best use of it to support your education at the School and prepare you for the wider world. There are important sections at the back that cover the legal and regulatory requirements that the School has to follow.

This is the acceptable use policy for all pupils of Stockport Grammar School (the **School**).

The aims of this policy are:

1.1.1 to educate and encourage you to make good use of the educational opportunities presented by access to technology;

1.1.2 to safeguard and promote your welfare, in particular by anticipating and preventing the risks arising from:

(a) exposure to harmful or inappropriate material (such as pornographic, racist, extremist or offensive materials);

(b) the sharing of personal data, including images;

(c) inappropriate online contact or conduct; and

(d) cyberbullying and other forms of abuse.

1.1.3 to minimise the risk of harm to the assets and reputation of the School;

1.1.4 to help you take responsibility for your own safe use of technology;

1.1.5 to ensure that you use technology safely and securely and are aware of both external and peer-to-peer risks when using technology; and

1.1.6 to prevent the unnecessary criminalisation of you or any other pupils.

2 Scope and application

This policy applies to the whole School including the Early Years Foundation Stage (**EYFS**).

This policy applies to you accessing the School's technology whether on or off School premises, or using your own or others' technology in a way which affects the welfare of any other pupil or member of the School community or where the culture or reputation of the School is put at risk.

Please encourage your Parents to read this policy; remember many of them will be learning about some of these things as well. The School actively promotes the participation of parents to help the School safeguard everyone's welfare and promote the safe use of technology.

3 Regulatory framework

Full details of the regulatory framework (the legal stuff) which identify what the school's responsibilities are can be found at the back in Appendix 5.

4 Publication and availability

This policy is published on the School website.

You can ask for a printed copy from the Bursary or go and ask to see a copy in the Bursary during the school day.

You can ask for this policy to be made available in large print or other accessible format if required.

5 Definitions

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:

5.1.1 the internet;

5.1.2 email;

5.1.3 mobile phones and smartphones;

5.1.4 desktops, laptops, netbooks, tablets / phablets and smartwatches;

5.1.5 personal music players;

5.1.6 devices with the capability for recording and / or storing still or moving images;

5.1.7 social networking, micro blogging and other interactive websites;

5.1.8 instant messaging (including image and video messaging via apps such as Snapchat and WhatsApp), chat rooms, blogs and message boards;

5.1.9 webcams, video hosting sites (such as YouTube);

5.1.10 gaming sites;

5.1.11 virtual learning environments such as SGS Online, Kerboodle, ActiveLearn. Show My Homework, GCSE Pod;

5.1.12 SMART boards; and

5.1.13 other photographic or electronic equipment e.g. GoPro devices.

6 Responsibility statement and allocation of tasks

The Governors of the School have overall responsibility for all matters which are the subject of this policy. Details as to how they will discharge these responsibilities are included in Appendix 6

7 Safe use of technology

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

The School will support everyone to develop their skills and make internet access as unrestricted as possible whilst balancing the safety and welfare of all the pupils and the security of the School's systems. The safe use of technology is integral to the School's curriculum. All pupils are educated about the importance of safe and responsible use of technology to help them to protect themselves and others online.

You may find the following resources helpful in keeping yourself safe online:

7.1.1 http://www.thinkuknow.co.uk/

7.1.2 http://www.childnet.com/young-people

7.1.3 https://www.saferinternet.org.uk/advice-centre/young-people

7.1.4 https://www.disrespectnobody.co.uk/

7.1.5 http://www.safetynetkids.org.uk/

7.1.6 http://www.childline.org.uk/Pages/Home.aspx

Please see the School's online safety policy for further information about the School's online safety strategy.

8 Internet and email

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

You can only access the School's network when given specific permission to do so. You will receive guidance on the use of the School's internet and email systems. If you are unsure about whether you are doing the right thing, you must seek assistance from a member of staff.

For everyone's protection, the use of email and of the internet will be monitored by the School. You should remember that even when an email or something that has been downloaded has been deleted, it can still be traced on the system. You should not assume that files stored on servers or storage media are always private.

9 School Rules

As part of the School Rules you **must** comply with the following rules and principles:

9.1.1 access and security (Section 1);

9.1.2 use of internet and email (Section 2);

9.1.3 use of mobile electronic devices (0); and

9.1.4 photographs and images (including "sexting") (0).

The purpose of these rules is to set out the principles which you must remember at all times and also the rules which you must follow to use technology safely and securely.

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

10 Procedures

You are responsible for your actions, conduct and behaviour when using technology at all times. Use of technology should be safe, responsible, respectful to others and legal. If you are aware of misuse you should talk to a teacher about it as soon as possible.

Any misuse of technology by you will be dealt with under the School's behaviour and discipline policy and where safeguarding concerns are raised, under the child protection and safeguarding policy and procedures.

You must not use your 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 you think that you might have been bullied or that someone else is being bullied, you should talk to a member of staff about it as soon as possible. See the School's anti-bullying policy for further information about cyberbullying and e-safety, including useful resources.

The Designated Safeguarding Lead (Mrs White in the Senior School and Mr Wheeler in the Junior School) takes lead responsibility within the School for safeguarding and child protection, including online safety. 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 child protection and safeguarding policy and procedures.

If you are worried about something that you have seen on the internet, or on any electronic device, including on another person's electronic device, you must tell a member of staff about it as soon as possible.

In a case where the pupil is considered to be vulnerable to radicalisation they may be referred to the Channel programme. 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.

In addition to following the procedures in the relevant policies as set out above, all serious incidents involving technology must be reported to the Designated Safeguarding Lead and if these involve the school's network or equipment the Network Manager will record the matter centrally in a technology incidents log.

11 Sanctions

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 Headmaster to apply any sanction which is appropriate and proportionate to the breach in accordance with the School's behaviour and discipline policy including, in the most serious cases, expulsion. Other sanctions might include: increased monitoring procedures; withdrawal of the right to access the School's network account; detention. Any action taken will depend on the seriousness of the offence.

Unacceptable use of technology could lead to the confiscation of a device or deletion of the material in accordance with the procedures in this policy and the School's Behaviour and Discipline policy (see Appendix 5 of the Behaviour and Discipline Policy for the School's policy on the searching and confiscation of electronic devices).

If there are reasonable grounds to suspect that the confiscated device contains evidence in relation to an offence, or that it contains a pornographic image of a child or an extreme pornographic image, the device will be given to the police. See Appendix 4 for more information on photographs and images.

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

12 Training

The School ensures that regular guidance and training for staff is arranged so that they understand what is expected of them by this policy and have the necessary knowledge and skills to carry out their roles.

The level and frequency of training depends on role of the individual member of staff.

The School maintains written records of all staff training.

13 Risk assessment

Where a concern about a pupil's welfare is identified, the risks to that pupil's welfare will be assessed and appropriate action will be taken to reduce the risks identified.

The format of risk assessment may vary and may be included as part of the School's overall response to a welfare issue, including the use of individual pupil welfare plans (such as behaviour, healthcare and education plans, as appropriate). Regardless of the form used, the School's approach to promoting pupil welfare will be systematic and pupil focused.

The Headmaster has overall responsibility for ensuring that matters which affect pupil welfare are adequately risk assessed and for ensuring that the relevant findings are implemented, monitored and evaluated.

14 Record keeping

All records created in accordance with this policy are managed in accordance with the School's policies that apply to the retention and destruction of records.

All serious incidents involving the use of technology will be logged centrally by the Designated Safeguarding Lead and where appropriate the Network Manager.

The records created in accordance with this policy may contain personal data about you. The School has a number of privacy notices which explain how the School will use personal data about pupils and parents. All pupils are given a copy of this and the privacy notices are published on the School's website. In addition, staff must ensure that they follow the School's data protection policies and procedures when handling personal data created in connection with this policy. This includes the School's data protection policy and information security policy.

15 Version control

Authorised by **Chairman of Governors**	Christopher Dunn
Date	25.06.2019

Circulation	Governors / teaching staff / all staff / parents / pupils / website

Section 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 without the express, prior consent of a member of staff.

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 You should only connect a school owned device to the school's network; 6th Form pupils can connect devices to the 6th Form guest WiFi. You must have written permission if you wish to bring and use your own device e.g a laptop.

4 You should only load material from external storage devices if you have created the material yourself or have taken all reasonable steps to make sure it is free from viruses.

The use of cellular data (e.g. GPRS, 3G, 4G, etc) to access the internet while pupils are on School premises or otherwise in the care of the School is discouraged, as pupils are unable to benefit from the School's filtering and anti-virus software. Pupils accessing the internet outside the School's network whilst on School premises or otherwise in the care of the School do so at their own risk and must comply with all the provisions of this policy regarding acceptable behaviour.

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. You must change your password each term or when instructed by the school and you should familiarise yourself with the guidance available at the time about establishing a safe password.

6 You must not attempt to gain unauthorised access to anyone else's computer or to confidential information which you are not authorised to access. If there is a problem with your passwords, you should speak to your form teacher or contact the IT Helpdesk

7 You must not attempt to access or share information about others without the permission of a member of staff. 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. If any problem with the School's network security is identified it must be reported to your form teacher or the IT Helpdesk as soon as possible.

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.

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 a member of the IT Helpdesk 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 pupils and to School security. The use of any website or application, whether on a School or personal device, with the capability of identifying the user's location while you are on School premises or otherwise in the care of the School is discouraged.

Section 2 Use of the internet and email

1 The School does not undertake to provide continuous internet access and reserves the right to change Email and website addresses with due notice.

Use of the internet

2 You must use the School's computer system for educational purposes only and are not permitted to access social media websites without the express, prior consent of a member of staff.

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 the Network Manager.

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) anyone else'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 are provided with your own personal email account for School purposes.

10 Your School email accounts can be accessed outside school via webmail on the School's website.

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 Headmaster 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 could also cause the School's network to suffer delays and / or damage.

15 A disclaimer will automatically be added to all outgoing correspondence from your School email account.

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

Section 3 Use of mobile electronic devices

1 **Mobile electronic device** includes but is not limited to mobile phones, smartphones, smartwatches tablets, laptops and MP3 players.

2 Mobile phones and other mobile electronic devices must be switched off (and not just on silent mode) and kept in bags during School hours, including before morning registration, at break times and between lessons. Use of such devices is only permitted during School hours with the express permission of a member of staff.

3 Pupils in the Sixth Form are permitted to use their mobile devices in the designated 6th Form areas via the appropriate WiFi points

4 The use of cellular data (e.g. GPRS, 3G, 4G, etc) to access the internet while you are on School premises or otherwise in the care of the School is discouraged, as you are unable to benefit from the School's filtering and anti-virus software. If you access the internet outside the School's network whilst on School premises or otherwise in the care of the School you do so at your own risk and must comply with all the provisions of this policy regarding acceptable behaviour.

5 The use of mobile phones during the School day will not be necessary. In emergencies, you may request to use the School telephone. Should your parents wish to contact you in an emergency, they will telephone the School office and a message will be relayed promptly.

6 You must not bring mobile electronic devices into examination rooms under any circumstances, except where special arrangements for the use of a laptop have been agreed with the Exams Officer of Head of learning Support in writing.

7 You must not communicate with staff using a mobile phone (or other mobile electronic device) except when this is expressly permitted by a member of staff, for example when necessary during an educational visit. Any such permitted communications should be brief and courteous.

8 Use of electronic devices of any kind to bully, harass, intimidate or attempt to radicalise others will not be tolerated and will constitute a serious breach of discipline, whether or not you are in the care of the School at the time of such use. Appropriate disciplinary action will be taken where the School becomes aware of such use (see the School's anti-bullying policy] and behaviour and discipline policy) and the School's safeguarding procedures will be followed in appropriate circumstances (see the School's child protection and safeguarding policy and procedures).

9 Mobile electronic devices may be confiscated and searched in appropriate circumstances. Please see Appendix 5 of the School's Behaviour and Discipline Policy] on the searching of electronic devices. You may also be prevented from bringing a mobile electronic device into the School temporarily or permanently and at the sole discretion of the Headmaster.

10 The School does not accept any responsibility for the theft, loss of, or damage to, mobile electronic devices brought onto School premises, including devices that have been confiscated or which have been handed in to staff.

Section 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 appearing in the image. If the material found is a pornographic image of a child or an extreme pornographic image this will not be deleted and the device will be delivered to the police, as stated in paragraph 11.3 of this policy.

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 Headmaster is considered to be offensive or which brings the School into disrepute on any form of social media or web services such as YouTube WhatsApp Instagram 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.

5 **Sexting**

5.1 **Sexting** means the taking and sending or posting of images or videos of a sexual or indecent nature of you or another pupil, usually through mobile picture messages or webcams over the internet.

5.2 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.

5.3 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 doing certain jobs in the future.

5.4 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.

5.5 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.

5.6 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.

5.7 Even if you don't share images 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.

5.8 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 child protection and safeguarding policy and procedures).

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

If sexual images or videos have been made and circulated online, you can be supported to get the images removed through the Internet Watch Foundation.

Appendix 1 The Legal Stuff

1. This policy has been prepared to meet the School's responsibilities under:

   1.1 Education (Independent School Standards) Regulations 2014;

   1.2 *Statutory framework for the Early Years Foundation Stage* (DfE, March 2017);]

   1.3 Education and Skills Act 2008;

   1.4 Children Act 1989;

   1.5 Childcare Act 2006;

   1.6 Data Protection Act 2018 and General Data Protection Regulation (GDPR) and

   1.7 Equality Act 2010.

2. This policy has regard to the following guidance and advice:

   2.1 Keeping children safe in education (DfE, September 2018);

   2.2 Preventing and tackling bullying (DfE, July 2017);

   2.3 Sexting in schools and colleges: responding to incidents and safeguarding young people (UK Council for Child Internet Safety, August 2016);

   2.4 Sexual violence and sexual harassment between children in schools and colleges (DfE, May 2018); and

   2.5 Searching, screening and confiscation: advice for schools (DfE, January 2018).

3. The following School policies, procedures and resource materials are relevant to this policy:

   3.1 behaviour and discipline policy;

   3.2 anti-bullying policy;

   3.3 online safety policy;

   3.4 expulsion and removal: review procedure;

   3.5 child protection and safeguarding policy and procedures; and

   3.6 risk assessment policy for pupil welfare.

Appendix 2: ACCEPTABLE USE AGREEMENT

This agreement is intended to encourage imaginative, responsible and safe use of digital technologies. By acting with care and thought pupils should be putting into practice much of this policy.
The School provides networked desktop computers with access to the internet through the School's own filtered connection. Wireless access is available for use by pupils in the 6th Form for their own devices.
It is standard practice in organisations to audit users' internet activity and all staff and pupils are audited in this way. Audit trails are examined when necessary. Should you find yourself looking at or opening material you consider the School would think inappropriate (or material you find disturbing), simply inform a member of staff so we can work with you to address the matter.

● I understand that the school will log and monitor my use of computers, devices and my digital communications

Identity and responsibility (online and digital)

This section applies to all your use of digital technologies, whether school-owned or personal.

In the digital realm, once something is posted online it has a persistence that is not like something that is said. It is also replicable and searchable (directly and through its metadata), and you cannot be sure who your audience is or will be. Once something is posted online, its effects are often magnified and can be mirrored out of context. All of this requires experience to understand. Remember: when you post, you have not only your own reputation to consider but also that of others and that of the School. Every member of the community has to take responsibility for his or her actions online. If you are in doubt, it is best not to post, send an email, etc.

● I will respect and maintain the integrity of my own and others' digital identities
● I will log on only as myself
● I will keep my login details private and make them secure
● I will not leave any device logged in and accessible to others
● I will exercise informed judgement about disclosing my personal details and will not give out another person's details without their clear consent
● I will be polite and responsible when I communicate with others.
● I will not make, post or send images and video footage of others except with the agreement and understanding of those involved. Agreement must extend to the finished, edited product
● I understand that the School's computers and systems are not to be used to upload, download or access any materials which are illegal, or which endorse, condone, or incite illegal, extremist or terrorist activity or which are in any other way inappropriate for school, or likely to cause harm or distress to others, or bring the School's name into disrepute. I understand that I may not use any program or software to access such materials by bypassing the School's filters.

Network and hardware integrity

I will respect and maintain the network and the computers the School provides:
● I will not open unexpected or suspicious files.

● I understand the need to exercise judgement when connecting a storage device (e.g. a USB drive) to the School's network. Any files will be material created for my school work and will have been created on a computer that has current anti-virus software.

● I will not link devices that are themselves computers (in whatever form) to the wired network without first consulting either the Director of Studies or the ICT team.

● I understand the need to exercise judgement when downloading files and am aware that viruses can be hidden in documents and images (for example) and not just in executable files. I will always seek advice if in doubt.

● I will respect the network's integrity when sending messages. I will not spam people or send needless messages. I will not attempt to send messages anonymously or pseudonymously for malicious purposes.

● I will report any actual or potential technical incident or security breach to my Form Teacher or the Network Manager.

● I understand that if I fail to observe this agreement I will be subject to disciplinary action.

I have read and agree to comply with the rules and regulations set out in the School's ICT Acceptable Use Policy for pupils.

Signed (pupil)

Name

Date

Signed (parent or guardian)

Name

Date