STOCKPORT GRAMMAR SCHOOL

IT ACCEPTABLE USE POLICY FOR STAFF

(Reviewed by Governors 13.10.20)

IT acceptable use policy

1. ***Introduction***: This policy sets out the requirements with which you must comply when using the School's IT and when otherwise using IT in connection with your job including:

    a. the School's email and internet services;

    b. telephones and faxes;

    c. the use of mobile technology on School premises or otherwise in the course of your employment (including 3G / 4G or Bluetooth or other wireless technologies), whether using a school or a personal device; and

    d. any hardware (such as laptops, printers or mobile phones) or software provided by, or made available by, the School.

    e. This policy also applies to your use of IT off school premises if the use involves Personal Data of any member of the School community or where the culture or reputation of the School are put at risk.

2. ***Failure to comply***: Failure to comply will constitute a disciplinary offence and will be dealt with under the School's disciplinary procedure.

3. ***Property***: You should treat any property belonging to the School with respect and reasonable care and report any faults or breakages immediately to the Network Manager or the Bursar. You should not use the School's computers or other IT resources unless you are competent to do so and should ask for training if you need it.

4. ***Viruses and other malicious code***: You should be aware of the potential damage that can be caused by computer viruses and other malicious code. You must not use, introduce or operate any hardware, programmes or data (including computer games) or open suspicious emails without permission from the Network Manager.

5. ***Passwords***: Passwords should be long, for example, you could use a song lyric or a memorable phrase plus a number. Do not choose a password which is so complex that it's difficult to remember without writing it down. Your password should not be disclosed to anyone else. In addition:

    a. your password should be difficult to guess, for example, you could base your password on something memorable that no one else would know. You should not use information which other people might know, or be able to find out, such as your address or your birthday;

    b. you must not use a password which is used for another account. For example, you must not use your password for your private email address or online services for any school account;

c. passwords (and any other security credential you are issued with such as a key fob or USB drive) must be kept secure and confidential and must not be shared with, or given to, anyone else. Passwords should not be written down.

d. You will be required to change your password at the start of each term; the IT department will give notification of the time of the change.

6. ***Leaving workstations***: If you leave your workstation for any period of time you should take appropriate action and, in particular, you should lock your screen to prevent access by others.

7. ***Concerns***: You have a duty to report any concerns about the use of IT at the School to the Bursar or Headmaster. For example, if you have a concern about IT security or pupils accessing inappropriate material.

8. ***Other policies***: This policy should be read alongside the following:

   a. Staff code of conduct;

   b. data protection policy for Staff;

   c. information security policy; and

   d. acceptable use policy for pupils

   e. online safety policy.

Internet

9. ***Downloading***: Downloading of any programme or file which is not specifically related to your job is strictly prohibited.

10. ***Personal use***: The School permits the incidental use of the internet so long as it is kept to a minimum and takes place substantially out of normal working hours. Use must not interfere with your work commitments (or those of others). Personal use is a privilege and not a right. If the School discovers that excessive periods of time have been spent on the internet provided by the School or it has been used for inappropriate purposes (as described in section 11 below), either in or outside working hours, disciplinary action may be taken and internet access may be withdrawn without notice at the discretion of the Headmaster.

11. ***Unsuitable material***: Viewing, retrieving or downloading of pornographic, terrorist or extremist material, or any other material which the School believes is unsuitable is strictly prohibited and constitutes gross misconduct. This includes such use at any time on the School's network, or via 3G or 4G when on School premises or otherwise in the course of your employment and whether or not on a School or personal device. Internet access may be withdrawn without notice at the discretion of the Headmaster whilst allegations of unsuitable use are investigated by the School.

12. ***Contracts***: You are not permitted to enter into any contract or subscription on the internet (including through an App) on behalf the School, without specific permission from the Bursar. This applies both to "free" and paid for contracts, subscriptions and Apps.

13. ***Retention periods***: the School keeps a record of staff browsing histories via Smoothwall monitoring normally for a period of one month.

Email

14. ***Personal use***: The School permits the incidental use of its email systems to send personal emails as long as such use is kept to a minimum and takes place substantially out of normal working hours. Personal emails should be labelled "personal" in the subject header. Use must not interfere with your work commitments (or those of others). Personal use is a privilege and not a right. The School may monitor your use of the email system, please see paragraphs 22 to 26 below, and staff should advise those they communicate with that such emails may be monitored. If the School discovers that you have breached these requirements, disciplinary action may be taken.

15. ***Status***: Email should be treated in the same way as any other form of written communication. Anything that is written in an email is treated in the same way as any form of writing. You should not include anything in an email which is not appropriate to be published generally.

16. ***Inappropriate use***: Any email message which is abusive, discriminatory on grounds of sex, marital or civil partnership status, age, race, disability, sexual orientation or religious belief (or otherwise contrary to our equal opportunities policy), or defamatory is not permitted. Use of the email system in this way constitutes gross misconduct. The School will take no responsibility for any offence caused by you as a result of downloading, viewing or forwarding inappropriate emails.

17. ***Legal proceedings***: You should be aware that emails are disclosable as evidence in court proceedings and even if they are deleted, a copy may exist on a back-up system or other storage area.

18. ***Jokes***: Trivial messages and jokes should not be sent or forwarded to the email system. They could cause the School's IT system to suffer delays and / or damage or could cause offence.

19. ***Contracts***: Contractual commitments via an email correspondence are not allowed without the prior authorisation of the Bursar.

20. ***Disclaimer***: All external correspondence by email should contain the School's disclaimer; this is normally applied automatically.

21. ***Data protection disclosures***: Subject to a number of limited exceptions, potentially all information about an individual may be disclosed should that individual make a Subject Access Request under data protection legislation. There is no exemption for embarrassing information (for example, an exchange of emails containing gossip about the individual will usually be disclosable). Staff must be aware that anything they put in an email is potentially disclosable.

Monitoring

22. The School regularly monitors and accesses its IT system for purposes connected with the operation of the School. The School IT system includes any hardware, software, email account, computer, device or telephone provided by the School or used for School business. The School will log and may also monitor staff use of the School telephone system and voicemail messages. Staff should be aware that the School will monitor the contents of a communication (such as the contents of an email).

23. The purposes of such monitoring and accessing include:

a. to help the School with its day to day operations. For example, if a member of staff is on holiday or is off sick, their email account may be monitored in case any urgent emails are received; and

b. to check staff compliance with the School's policies and procedures and to help the School fulfil its legal obligations. For example, to investigate allegations that a member of staff has been using their email account to send abusive or inappropriate messages.

24. Monitoring may be carried out on a random basis and it may be carried out in response to a specific incident or concern.

25. The School also uses software which automatically monitors the School IT system (for example, it would raise an alert if a member of Staff sent an email containing an inappropriate word or phrase).

26. The monitoring is carried out automatically. If anything of concern is revealed as a result of such monitoring then this information may be shared with the Deputy Head, Headmaster or Designated Safeguarding Lead and this may result in disciplinary action. In exceptional circumstances concerns will need to be referred to external agencies such as the Police.

ONLINE SAFETY POLICY - APPENDIX

Online Safety Arrangements During

Remote Learning due to Coronavirus

Context

It is more important than ever that the School continues to provide a safe environment, including online.

This is an appendix to the School's Online Safety Policy, IT Acceptable Use Policy for Staff, IT Acceptable Use Policy for Pupils, Data Protection Policy and Information Security Policy. This appendix summarises key COVID 19 related changes or additions.

We will continue to ensure that appropriate filters and monitoring systems are in place to protect pupils when they are online on our IT systems or recommended resources.

The person in charge of maintaining safe IT arrangements in the School is Mr Flaherty and he can be contacted by email on ictcoordinator@stockportgrammar.co.uk

Should the School's IT staff become unavailable, we will publish contingency arrangements to ensure the safety and stability of our IT provision.

Pupils should continue to follow our normal policies and procedures whether working in school or remotely at home.

1 Remote learning arrangements

The same principles as set out in the School's Safeguarding Policy and Pupil Behaviour and Discipline Policy apply to all online interactions between staff and pupils.

Appendix 4 of the School's Safeguarding Policy (Staff Code of Conduct) already includes provision relating to staff/pupil relationships and communication using technology. This Code of Conduct also applies to remote learning.

Remote learning will be delivered via the following platforms/facilities which have been evaluated and agreed by the School's Senior Management Team:

- Show My Homework
- Google Classroom
- Google Meet (live and recorded)
- Classlist
- Tapestry
- School email accounts

2 Role of parents

Parents have responsibility for ensuring appropriate supervision when their children are working online and that appropriate online parent controls are in place.

The following are suitable online safety resources for parents:

- Coronavirus (COVID-19): support for parents and carers to keep children safe online provides guidance from the government
- Coronavirus (COVID-19) - staying safe online provides guidance from the government
- Thinkuknow provides advice from the National Crime Agency (NCA) on staying safe online

- Parent info is a collaboration between Parent Zone and the NCA providing support and guidance for parents from leading experts and organisations
- Childnet toolkit is a toolkit to support parents to start discussions about online behaviour
- UK Safer Internet Centre has advice for parents to help keep children safe online
- Internet matters provides guides on how to set parental controls on a range of devices
- Net-aware has guides for parents on social networks, apps and games
- London Grid for Learning has support for parents to keep their children safe online
- Let's Talk About It has advice for parents to keep children safe from online radicalisation

3 Safeguarding arrangements

The School's arrangements for reporting safeguarding concerns are set out in the School's Safeguarding Policy.

Pupils and parents can also access help and support at:

- UK Safer Internet Centre 'Report Harmful Content' to report harmful content
- CEOP (National Crime Agency Child Exploitation and Online Protection Command to report online abuse
- Educate Against Hate for government advice on safeguarding from radicalisation

4 Staff training

Staff have been given training on the use of the online platforms/facilities that the school is using. Updates to this training are provided as necessary.

Authorised by Chairman of Governors	Christopher Dunn
Date	13.10.2020

Circulation	Governors / teaching staff / all staff / parents / website
Status	Regulatory