Stretford Grammar School

Aspirat primo fortuna labori

E-Safety Policy

Ratified by Governors : March 2017

E-SAFETY POLICY

Date of Review: January 2019

Member of staff with overall responsibility: Mr D.Price-Uden

Purpose	This document outlines the commitment of Stretford Grammar School to ensuring the eSafety of our students and staff and in preparing our students for the use of technology in the future. It also provides guidance to staff to ensure the safeguarding needs of our students are met at all times by: • Protecting and educating staff and students in the safe use of technology • Implementing appropriate mechanisms to intervene and support any incidents, where appropriate • Enforcing relevant legislation and upholding best practice

Document History	This policy is based on the guidance document developed by Hertfordshire Grid for Learning (http://www.thegrid.org.uk/eservices/safety/policies.shtml).

Contents

1. Introduction

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Apps
- E-mail, Instant Messaging and chat rooms
- Social Media, including Facebook and Twitter
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices including tablets and gaming devices
- Online Games
- Learning Platforms and Virtual Learning Environments
- Blogs and Wikis
- Podcasting
- Video sharing
- Downloading of all content
- On demand TV and video, movies and radio / Smart TVs

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies and that some have minimum age requirements (13 years in most cases).

At Stretford Grammar School, we understand the responsibility to educate our students on eSafety Issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Schools hold personal data on learners, staff and others to help them conduct their day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, and potentially damage the reputation of the school. This can make it more difficult for your school to use technology to benefit learners.

Everybody in the school community has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

This policy is inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, smartphones, tablets, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by students and staff, but brought onto school premises (such as laptops, mobile phones, smartphones and portable media players, etc "Bring Your Own Device" (BYOD)).

This policy is based on the guidance document developed by Hertfordshire Grid for Learning, which can be found here:
http://www.thegrid.org.uk/eservices/safety/policies.shtml

Other material from additional sources is credited where relevant.

Both this policy and the Acceptable Use Agreement (for all staff, governors, regular visitors [for regulated activities] and students) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, mobile devices, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by students and staff, but brought onto school premises (such as laptops, mobile phones and other mobile devices).

2. Monitoring

Authorised ICT staff may inspect any ICT equipment owned or leased by the school at any time without prior notice. ICT authorised staff may monitor, intercept, access, inspect, record and disclose telephone calls, e-mails, instant messaging, internet/intranet use and any other electronic communications (data, voice, video or image) involving its employees or contractors, without consent, to the extent permitted by law. This may be to confirm or obtain school business related information; to confirm or investigate compliance with school policies, standards and procedures; to ensure the effective operation of school ICT; for quality control or training purposes; to comply with a Subject Access Request under the Data Protection Act 1998, or to prevent or detect crime.

ICT authorised staff may, without prior notice, access the e-mail or voice-mail account where applicable, of someone who is absent in order to deal with any business-related issues retained on that account.

All monitoring, surveillance or investigative activities are conducted by ICT authorised staff and comply with the Data Protection Act 1998, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000.

Please note that personal communications using School ICT may be unavoidably included in any business communications that are monitored, intercepted and/or recorded.

3. eSafety

3.1 Roles and Responsibilities

As eSafety is an important aspect of strategic leadership within the school, the Head and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named eSafety co-ordinator in this school is David Price-Uden who has been designated this role as a member of the Senior Leadership team. In addition the network manager, James Keating, is responsible for ensuring that all eSafety network protocols are in place, monitored and updated as necessary. All members of the school community have been made aware of who holds this post. It is the role of the eSafety co-ordinator to keep abreast of current issues and guidance through organisations such as LA,TSCB, CEOP (Child Exploitation and Online Protection) and Childnet.

Senior Management and governors are updated by the Head/ eSafety co-ordinator and all governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

This policy, supported by the school's acceptable use agreements for staff, governors, visitors and students, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: Safeguarding, Health and Safety, Behaviour and Staff Code of Conduct.

3.2 eSafety in the Curriculum

ICT and online resources are increasingly used across the curriculum. It is essential for eSafety guidance to be given to the students on a regular and meaningful basis. eSafety is embedded within our curriculum and we continually look for new opportunities to promote eSafety.

The school has a framework for teaching internet skills in Computing and PSCHE lessons – for instance eSafety resources from CEOP (covering Internet safety, cyber bullying and related issues) are be embedded in the curriculum and delivered to all year groups.

Educating students about the online risks that they may encounter outside school is done informally when opportunities arise and as part of the eSafety curriculum and in assemblies and year group information evenings delivered to parents.

Students are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them.

Students are taught about copyright, respecting other people's information, safe use of images and other important areas through discussion, modeling and appropriate activities.

Students are aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. Students are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Childline or the 'CEOP report' button (the school website home page has a direct link to the CEOP homepage with the 'Make a Report' link).

3.3 eSafety Skills Development for Staff

New staff receive information on the school's acceptable use policy as part of their induction.

All staff have been made aware of their individual responsibilities relating to the safeguarding of children within the context of eSafety and know what to do in the event of misuse of technology by any member of the school community (see eSafety Coordinator)

All staff are encouraged to incorporate eSafety activities and awareness within their curriculum areas and ensure they are adequately informed with up-to-date areas of concern.

3.4 Managing the School eSafety Messages

We endeavour to embed eSafety messages across the curriculum whenever the internet and/or related technologies are used.

The eSafety policy will be introduced to the students at the start of each school year.

The school website reflects information and guidance from key organisations such as Thinkuknow, Digital Parenting, CEOP, Wise Kids, KidSMART, Childnet and KnowItAll.

4. Staff Professional Responsibilities

Below is a clear summary of professional responsibilities related to the use of ICT which has been endorsed by unions (in association with Hertfordshire Grid for Learning). A copy is disseminated for display in all office spaces throughout the school.

Professional Responsibilities

When using any form of ICT, including the Internet in school and outside school, for your own protection, we advise that you:

- Ensure all electronic communication with students, parents, carers, staff and others is compatible with your professional role and in line with school policies.
- Do no talk about your professional role in any capacity when using social media such as Facebook and YouTube.
- Do not put online any text, image, sound or video that could upset or offend any member of the whole school community or be incompatible with your professional role.
- Use school ICT systems and resources for all school business. This includes your school e-mail address or school mobile phone and school video camera.
- Do not give out your own personal details, such as mobile phone number, personal e-mail address or social network details to students, parents, carers and others.
- Do not disclose any passwords and ensure that personal data (such as data held on SIMS) is kept secure and used appropriately.
- Only take images of students and/or staff for professional purposes, in accordance with school policy and with the knowledge of SLT.
- Do not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Ensure that your online activity, both in school and outside school, will not bring the school or our professional role into disrepute.
- You have a duty to report any eSafety incident which may impact on you, your professionalism or the school.

Stretford Grammar School

5. Data Security

The accessing and appropriate use of school data is taken very seriously. The school gives relevant staff access to its Management Information System, with a unique username and password.

It is the responsibility of everyone to keep passwords secure.

Staff must be aware of their responsibility when accessing school data and must follow the guidance. Staff are subject to guidance provided in the Policy for ICT Acceptable Use. A central record of signed Acceptable Use policies is held by the Network Manager.

Staff must keep all school related data secure. This includes all personal, sensitive, confidential or classified data.

Staff should avoid leaving any portable or mobile ICT equipment or removable storage media in unattended vehicles. Where this is not possible, keep it locked out of sight.

Staff should always carry portable and mobile ICT equipment or removable media as hand luggage, and keep it under your control at all times.

It is the responsibility of individual staff to ensure the security of any personal or sensitive information contained in documents faxed, copied, scanned or printed. This is particularly important when shared printers/copiers (multi-function print, fax, scan and copiers) are used.

5.1 Passwords

Always use your own personal passwords and make sure you enter your personal passwords each time you logon. Do not include passwords in any automated logon procedures.

Change passwords whenever there is any indication of possible system or password compromise and when indicated to do so by the Network Manager.

Do not record passwords or encryption keys on paper or in an unprotected file.

Only disclose your personal password to authorised ICT support staff when necessary, and never to anyone else. Ensure that all personal passwords that have been disclosed are changed once the requirement is finished.

Never tell a child or colleague your password. If you aware of a breach of security with your password or account inform the Network Manager immediately. If you think your password may have been compromised or someone else has become aware of your password report this to your ICT support team.

Passwords must contain a minimum of six characters and be difficult to guess.

Passwords should contain a mixture of upper and lowercase letters, numbers and symbols.

User ID and passwords for staff and students who have left the school are removed from the system as soon as is reasonably practical.

5.2 Password Security

Password security is essential for staff, particularly as they are able to access and use student data. Staff are expected to have secure passwords which are not shared with anyone. The students are expected to keep their passwords private and not to share with others, particularly their friends. Staff and students are regularly reminded of the need for password security.

All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's e-Safety Policy and Data Security.

Users are provided with an individual network, e-mail and Management Information System (SIMS) log-in username.

Students are not permitted to deliberately access on-line materials or files on the school network or local storage devices of their peers, teachers or others.

Staff are aware of their individual responsibilities to protect the security and confidentiality of the school networks, MIS systems and/or learning platform, including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations are not left unattended and are locked. The automatic log-off time for the school network is 135 minutes.

5.3 Protecting Personal or Sensitive Information

Ensure that any school information accessed from your own PC or removable media equipment is kept secure, and remove any portable media from computers when not attended.

Ensure you lock your screen before moving away from your computer during your normal working day to prevent unauthorised access.

Ensure the accuracy of any personal or sensitive information you disclose or share with others.

Ensure that personal, sensitive, confidential or classified information is not disclosed to any unauthorised person.

Ensure the security of any personal or sensitive information contained in documents you fax, copy, scan or print. This is particularly important when shared printers/copiers (multi-function print, fax, scan and copiers) are used and when access is from a nonschool environment.

Only download personal data from systems if expressly authorised to do so by your manager.

You must not post on the internet personal or sensitive information, or disseminate such information in any way that may compromise its intended restricted audience.

Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information.

Ensure hard copies of data are securely stored and disposed of after use.

5.4 Storing/Transferring Personal or Sensitive Information Using Removable Media

Ensure removable media is purchased with encryption.

Store all removable media securely.

Securely dispose of removable media that may hold personal data.

Encrypt all files containing personal or sensitive data.

Ensure hard drives from machines no longer in service are removed and stored securely or wiped clean.

5.5 Remote Access

Staff are responsible for all activity via the remote access facility.

Staff must only use equipment with an appropriate level of security for remote access.

To prevent unauthorised access to school systems, keep all dial-up access information such as telephone numbers, logon IDs and PINs confidential and do not disclose them to anyone.

Avoid writing down or otherwise recording any network access information. Any such information that is written down must be kept in a secure place and disguised so that no other person will be able to identify what it is.

Protect school information and data at all times, including any printed material produced while using the remote access facility. Take particular care when access is from a non-school environment.

5.6 Internet Access

The internet is an open worldwide communication medium, available to everyone, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. All internet use through the Stretford Grammar School network monitored. The network monitoring software packages, SMOOTHWALL and Impero, are used to provide reports on internet searches and alerts are sent to the DSL (Designated Safeguarding Lead: D. Price-Uden) and the Network Manager (J. Keating). Whenever any inappropriate use is detected it will be followed up. The reporting criteria that monitors network usage has been aligned with DFE guidance on the key word searches as outlined by the Prevent Agenda – CONSENT. Staff have received Prevent training and understand the referral process (see appendices).

5.7 Managing the Internet

The school provides students with supervised access to Internet resources (where reasonable) through the school's fixed and mobile internet connectivity.

Staff will preview any recommended sites, online services, software and apps before use.

Searching for images through open search engines is discouraged when working with students.

If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work.

All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.

All users must observe copyright of materials from electronic resources.

5.8 Internet Use

You must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise the intended restricted audience.

Do not reveal names of colleagues, students, others or any other confidential information acquired through your job on any social networking site or other online application.

On-line gambling or gaming is not allowed.

6. Infrastructure

At Stretford Grammar School the following web filtering protocols and systems are in place:

The school uses strict Software Restriction Policies to disallow any unknown software from running. This reduces the chances of any kind of virus or malicious software threat heavily by closing the usual points of entry.

Staff and students are aware that school based e-mail and internet activity can be monitored and explored further if required.

The school does not allow students access to internet logs.

The school uses management control tools for controlling and monitoring workstations.

If staff or students discover an unsuitable site, the screen must be switched off/closed and the incident reported immediately to the e-safety coordinator or teacher as appropriate.

Anti-virus protection is installed and kept up-to-date on all school machines.

7. E-mail

The use of e-mail within most schools is an essential means of communication for both staff and students. In the context of school, e-mail should not be considered private. Educationally, e-mail can offer significant benefits including; direct written contact between schools on different projects, be they staff based or student based, within school or international. We recognise that students need to understand how to style an e-mail in relation to their age and how to behave responsible online.

7.1 Managing e-mail

The school gives all staff their own e-mail account to use for all school business as a work based tool. This is to protect staff, minimise the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal profile information being revealed.

Staff should use their school e-mail for all professional communication.

It is the responsibility of each account holder to keep their password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary

e-mail histories can be traced. The school e-mail account should be the account that is used for all school business.

Under no circumstances should staff contact students, parents or conduct any school business using personal e-mail addresses.

A standard disclaimer is attached to all e-mail correspondence, stating that: "This email and its attachments are confidential and are intended for the above named recipient only. If this has come to you in error, please notify the sender immediately and delete this e-mail from your system. You must take no action based on this, nor must you copy or disclose it or any part of its contents to any person or organisation.

Statements and opinions contained in this e-mail may not necessarily represent those of the Governing Body of Stretford Grammar School. The School may be required to disclose this e-mail [or any response to it] under the Freedom of Information Act 2000, unless the information in it is covered by one of the exemptions in the Act.

This e-mail message has been checked for the presence of computer viruses, however we advise that in keeping with good IT practice the recipient should ensure that the e-mail together with any attachments are checked for viruses. We cannot accept any responsibility for any damage or loss caused by software viruses. 'the views expressed are not necessarily those of the school or the LA".

All e-mails should be written and checked carefully before sending, in the same way as a letter written on school headed paper.

Students may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes.

All student e-mail users are expected to adhere to the generally accepted rules of responsible online behaviour particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission, virus checking attachments.

Students must immediately tell a teacher/trusted adult if they receive an offensive or upsetting e-mail.

Staff must inform (the eSafety coordinator or line manager) if they receive an offensive e-mail.

Students receive access to their own e-mail account through Office 365. However you access your school e-mail (whether directly, through webmail when away from the office or on non-school hardware) all the school e-mail policies apply.

7.2 Sending e-mails

If sending e-mails containing personal, confidential, classified or financially sensitive data to external third parties or agencies, refer to the Section

7.3 Receiving e-mails

E-mail should be checked regularly and deleted or moved to another folder.

Never open attachments from an untrusted source; consult your network manager first.

Do not use the e-mail systems to store attachments. Detach and save business related work to the appropriate shared drive/folder.

The automatic forwarding and deletion of e-mails is not allowed.

7.4 E-mailing Personal or Confidential Information

Use your own school e-mail account so that you are clearly identified as the originator of a message.

School e-mail is not to be used for personal advertising.

Where your conclusion is that e-mail must be used to transmit such data:

Obtain express consent from your manager to provide the information by e-mail and exercise caution when sending the e-mail and always follow these checks before releasing the e-mail:

- Encrypt and password protect. See http://www.thegrid.org.uk/info/dataprotection/#securedata
- Verify the details, including accurate e-mail address, of any intended recipient of the information. ○ Verify (by phoning) the details of a requestor before responding to email requests for information. ○ Do not copy or forward the e-mail to any more recipients than is absolutely necessary.

Do not send the information to any person whose details you have been unable to separately verify (usually by phone).

Do not send the information as an encrypted document **attached** to an e-mail.

Provide the encryption key or password by a **separate** contact with the recipient(s).

Do not identify such information in the subject line of any e-mail.

Request confirmation of safe receipt.

8. Safe Use of Images

Taking of Images and Film:

Digital images are easy to capture, reproduce and publish and, therefore, misuse. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness. HCC guidance can be found here: http://www.thegrid.org.uk/eservices/safety/policies.shtml#images

With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment.

Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on field trips. However, with the express permission of the Headteacher, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the staff device.

Staff must not post any images of students on their personal network sites, including all social media sites.

Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of pupils, staff and others without advance permission from the Headteacher.

Pupils and staff must have permission from the Headteacher before any image can be uploaded for publication.

8.1 Publishing Pupil's Images and Work

On a child's entry to the school, all parents/carers will be asked to give permission to use their child's work/photos in the following ways:

- on the school web site
- in the school prospectus and other printed publications that the school may produce for promotional purposes
- recorded/ transmitted on a video or webcam
- on the school's learning platform or Virtual Learning Environment
- in display material that may be used in the school's communal areas
- in display material that may be used in external areas, i.e. exhibition promoting the school
- general media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, e.g. divorce of parents, custody issues, etc.
Parents or carers may withdraw permission, in writing, at any time. Consent must also be given in writing and will be kept on record by the school.

Pupils' names will not be published alongside their image and vice versa. E-mail and postal addresses of pupils will not be published. Pupils' full names will not be published.

Before posting student work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed.

Only the ICT Manager or members of SLT have authority to upload to the internet.

8.2 Storage of Images

Images/ films of students are stored on the school's network.

Students and staff are not permitted to use personal portable media for storage of images (eg, USB sticks) without the express permission of the Headteacher.

Rights of access to this material are restricted to the teaching staff and students within the confines of the school network or other online school resource.

9. Social Media, including Facebook and Twitter

Facebook, Twitter and other forms of social media are increasingly becoming an important part of our daily lives.

Staff are able to setup Social Learning Platform accounts, using their school e-mail address, in order to be able to teach students the safe and responsible use of Social Media.

Students are not permitted to access their social media accounts whilst at school.

Staff, governors, students, parents and carers are regularly provided with information on how to use social media responsibly and what to do if they are aware of inappropriate use by others.

Staff, governors, students, parents and carers are aware that the information, comments, images and video they post online can be viewed by others, copied and stay online forever.

Staff, governors, students, parents and carers are aware that their online behaviour should at all times be compatible with UK law.

10. Breaches

A breach or suspected breach of policy by a school employee, contractor or student may result in the temporary or permanent withdrawal of school ICT hardware, software or services from the offending individual.

For staff any policy breach is grounds for disciplinary action in accordance with the school Disciplinary Procedure.

For students, any policy breach will be dealt with according to the school's Behaviour, Rewards and Sanctions Policy.

Policy breaches may also lead to criminal or civil proceedings.

10.1 Misuse and Infringements

10.1.1 Complaints

Complaints and/ or issues relating to eSafety should be made to the eSafety coordinator or Headteacher. Incidents should be logged and the Stretford Grammar School Referral Flowchart for Managing an eSafety Incident should be followed. Incidents are logged on CPOMS.

10.1.2 Inappropriate Material

All users must report accidental access to inappropriate materials. The breach must be immediately reported to the eSafety co-ordinator.

Deliberate access to inappropriate materials by any user will lead to the incident being logged by the relevant responsible person, and an investigation by the Headteacher or their designated representative. Depending on the seriousness of the offence, sanctions could include immediate suspension, possibly leading to dismissal and involvement of police for very serious offences.

Users are made aware of sanctions relating to the misuse or misconduct through the Acceptable Use agreement.

10.1.3 Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's ICT Manager. Additionally, all security breaches, lost/stolen equipment or data (including remote access), virus notifications, unsolicited e-mails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the relevant responsible person. The relevant responsible individuals in the school are as follows:

David Price-Uden, Assistant Headteacher James Keating, ICT Manager.

11. School ICT Equipment including Portable & Mobile ICT Equipment & Removable Media

11.1 School ICT Equipment

As a user of the school ICT equipment, you are responsible for your activity.

Do not allow visitors to plug their ICT hardware into the school network points (unless special provision has been made). They should be directed to the wireless ICT facilities if available
Ensure that all ICT equipment that you use is kept physically secure.

Do not attempt unauthorised access or make unauthorised modifications to computer equipment, programs, files or data. This is an offence under the Computer Misuse Act 1990.

It is imperative that you save your data on a frequent basis to the school's network. You are responsible for the backup and restoration of any of your data that is not held on the school's network.

Personal or sensitive data should not be stored on the local drives of desktop PC, laptop, USB memory stick or other portable device. If it is necessary to do so the local drive must be encrypted.

On termination of employment, resignation or transfer, return all ICT equipment to your Manager. You must also provide details of all your system logons so that they can be disabled.

It is your responsibility to ensure that any information accessed from your own PC or removable media equipment is kept secure, and that no personal, sensitive, confidential or classified information is disclosed to any unauthorised person.

11.2 Portable & Mobile ICT Equipment

This section covers such items as laptops, mobile devices and removable data storage devices. Please refer to the relevant sections of this document when considering storing or transferring personal or sensitive data.

All activities carried out on school systems and hardware will be monitored in accordance with the general policy.

Staff must ensure that all school data is stored on the school network, and not kept solely on the laptop. Any equipment where personal data is likely to be stored must be encrypted.

Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes. When travelling by car, best practice is to place the laptop in the boot of your car before starting your journey.

Synchronise all locally stored data, including diary entries, with the central school network server on a frequent basis.

Ensure portable and mobile ICT equipment is made available as necessary for antivirus updates and software installations, patches or upgrades.

The installation of any applications or software packages must be authorised by the ICT support team, fully licensed and only carried out by your ICT support.

In areas where there are likely to be members of the general public, portable or mobile ICT equipment must not be left unattended and, wherever possible, must be kept out of sight. Portable equipment must be transported in its protective case if supplied.

11.3 Mobile Technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for students and young people. Mobile technologies such Smartphones, Blackberries, iPads, games players, are generally very familiar to students outside of school. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

11.4 Personal Mobile Devices (including phones)

The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the school allow a member of staff to contact a student or parent/carer using their personal device. Whilst on a school trip, there may be occasions when the use of a personal mobile phone is needed – this must be for emergency use only and staff accompanying the trip must be informed that a call will be made.

The school recognises that many parents and students wish students to have a personal mobile phone with them for the journey to and from school. Students are allowed to bring personal mobile devices/phones to school but must not use them during the school day. At all times the device must be switched off or onto silent.

The school is not responsible for the loss, damage or theft of any personal mobile device.

The sending of inappropriate text messages between any members of the school community is not allowed.

Permission must be sought before any image or sound recordings are made on these devices of any member of the school community.

Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

11.5 School Provided Mobile Devices (including phones)

The sending of inappropriate text messages between any members of the school community is not allowed.

Permission must be sought before any image or sound recordings are made on the devices of any member of the school community.

Where the school provides mobile technologies such as phones, laptops and iPads for offsite visits and trips, only these devices should be used. In the case of an emergency whereby the school device is incapacitated, members of staff should consult each other and agree upon an appropriate way in which to communicate with parents/carers. This may necessitate the use of a personal mobile.

Where the school provides a laptop for staff, only this device may be used to conduct school business outside of school.

11.6 Webcams and CCTV

The school uses CCTV in some areas for security and safety. The only people with access to this are the Network Manager, Headteacher and Designated Safeguarding Lead.

We do not use publicly accessible webcams in school.

Webcams will not be used for broadcast on the internet without prior parental consent. Misuse of a webcam by any member of the school community will result in sanctions (as listed under the 'inappropriate materials' section of this document)

Webcams include any camera on an electronic device which is capable of producing video. School policy should be followed regarding the use of such personal devices.

11.7 Managing Other Online Technologies

Online technologies, including social networking sites, if used responsibly both outside and within an educational context can provide easy to use, creative, collaborative and free facilities. However it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our students to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

At present, the school endeavours to deny access to social networking and online games websites to students within school – through webfiltering and monitoring via Smoothwall and Impero software packages.

All students are advised to be cautious about the information given by others on such websites, for example users not being who they say they are. Students are taught to avoid placing images of themselves (or details within images that could give background details) on such websites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.

Students are always reminded to avoid giving out personal details on websites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/ e-mail address, specific hobbies/ interests).

Our students are advised to set and maintain their online profiles to maximum privacy and deny access to unknown individuals.

Students are encouraged to be wary about publishing specific and detailed private thoughts and information online. Our students are asked to report any incidents of Cyberbullying to the school.

12. Parental Involvement

We believe that it is essential for parents/carers to be fully involved with promoting eSafety both in and outside of school and to be aware of their responsibilities.

Parents/carers are asked to read through and sign Acceptable Use agreements on behalf of their student on admission to the school.

Parents/carers are required to make a decision as to whether they consent to images of their student being taken and used in the public domain (eg. on school website).

13. Further help and support

Our organisation has a legal obligation to protect sensitive information under the Data Protection Act 1998.

For more information visit the website of the Information Commissioner's Office https://ico.org.uk/

Advice on eSafety - http://www.thegrid.org.uk/eservices/safety/index.shtml

Further guidance -
http://www.thegrid.org.uk/info/dataprotection/index.shtml#securedata

School's toolkit is available - Record Management Society website – http://www.rms-gb.org.uk/resources/848

Test your online safety skills http://www.getsafeonline.org

Data Protection Team – e-mail - data.protection@trafford.gov.uk

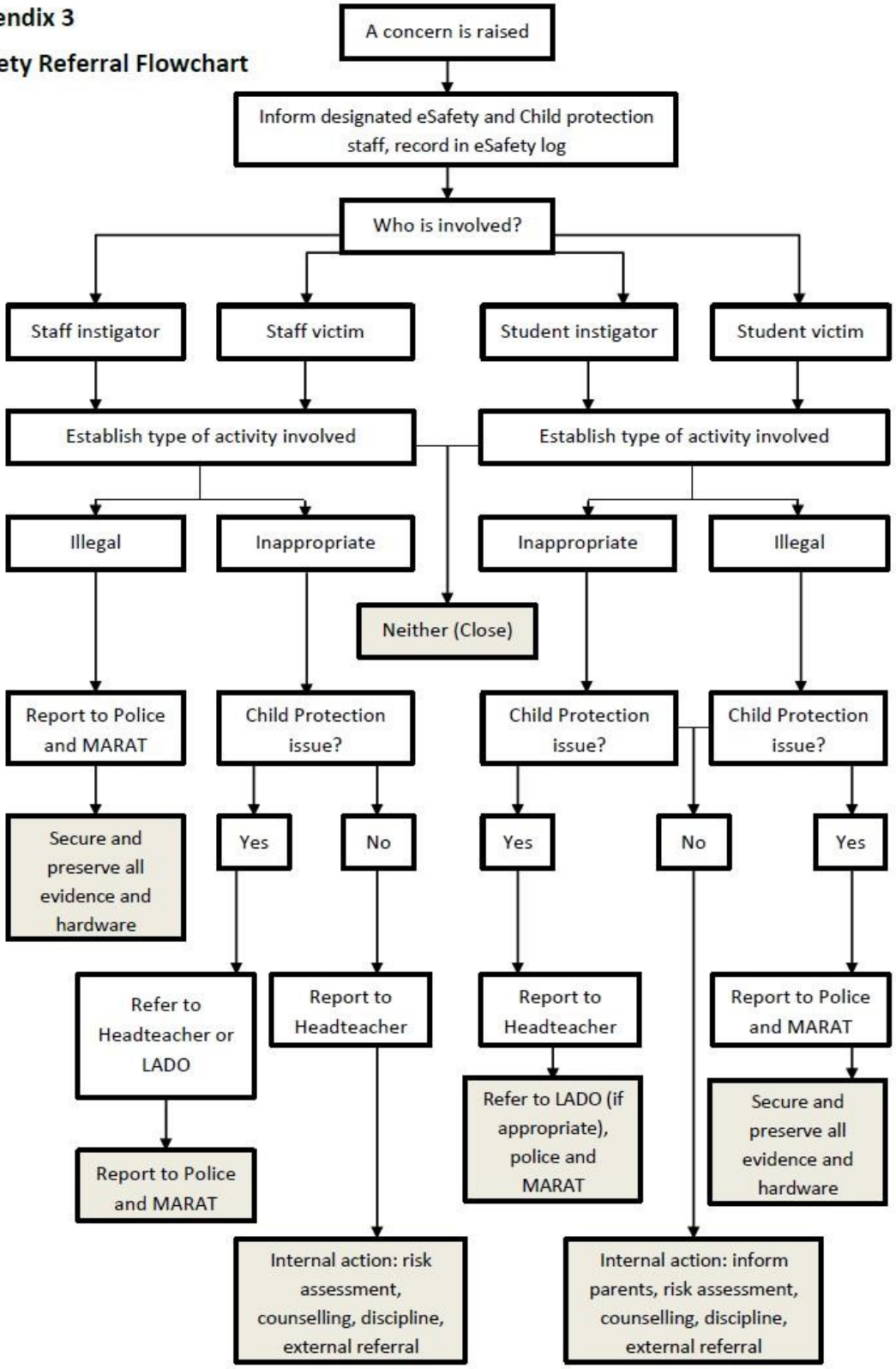
Information Commissioner's Office – www.ico.org.uk

14. Appendices eSafety

Referral Flowchart

Appendix 3

eSafety Referral Flowchart



Acceptable Use Agreement: Staff, Governors and Visitors

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which

open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and increase effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of ICT in their everyday work.
- The school will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for students/pupils learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that students/pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety:

- I understand and consent that the school may monitor and record my use of school ICT systems for the purpose of ensuring that the School's rules are being complied with and for legitimate business purposes. The school e-mail system will only be monitored for a particular user by direct request to the ICT Network Manager from the Headteacher.
- I understand that the school ICT systems are primarily intended for educational use and I will only use the School's Email/Internet/Intranet/Learning Platform and any related technologies for professional purposes. Use of the schools system for personal use is authorised but only at times that do not conflict with the working practices of the school.
- I will not install any hardware or software onto the school system (including school laptops) without the permission of the ICT Network Manager. If you require software or hardware to be installed, this is to be requested through the schools ICT Helpdesk.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (e.g.laptops, e-mail, VLE etc) out of school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- I will immediately report any illegal, inappropriate or harmful material or incident I become aware of, to the school's Designated Safeguarding Lead Mr Price-Uden.

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner. I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use my personal Stretford Grammar School equipment to record these images, unless I have permission to do so (Staff may obtain permission from the ICT Network Manager to use specific equipment on each occasion where the equipment will be used). Where these images are published (e.g. on the school website/VLE) it will not be possible to identify by name, or other personal information, those who are featured. There may be occasions where this rule cannot be applied, i.e. Newspaper articles, school newsletters and bulletins. In the event of this, prior approval should be obtained from the Headteacher.
- I will only communicate with students/pupils and parents/carers using official school systems. Any such communication will be professional in tone and manner. I will not communicate confidential information by e-mail.
- I will not engage in any on-line activity that may compromise my professional responsibilities. The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:
- If I use my personal hand held / external devices (tablets / laptops / USB devices /Smartphones etc) that connect to the school network, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- The school will provide staff with an e-mail account. This account is to be used for school business only. Staff must not use the school e-mail account for personal banking, online shopping etc. Access to personal e-mail accounts (I.E. Hotmail, AOL etc) using the school system is authorised, but staff are advised that they must not use their personal e-mail account to contact parents, carers, students etc
- I will not open any attachments to e-mails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will ensure that any school data held outside of the school network (I.E. USB pens, Mobile drives etc) is regularly backed up.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads from the internet that might take up internet capacity and prevent other users from being able to carry out their work. A large download is a file, program, movie etc that is over 500MB in size. If you require a download over this size

please contact ICT (via the ICT Helpdesk) who will arrange to download for you.

- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless given permission to do so by the ICT Network Manager.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others. I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School / LA Personal Data Policy (or other relevant school policy). Where personal data is transferred outside the secure school network, every effort should be made to make sure that it is encrypted. The school is currently investigating providing staff with resources to achieve this.
- I understand that data protection policy requires that any staff or student/pupil data, to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).
- I understand that I am responsible for my actions in and out of school relating to this policy.
- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and/or the Local Authority and in the event of illegal activities the involvement of the police. I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff Name:

Signed:

Date: