Sydenham School

E-Safety Policy

Updated October 2018

To be reviewed October 2020

1. Context:

1.1. E-Safety is designed to keep children and young people safe while they are accessing the internet, viewing blogs, watching videos, talking or posting on social media networks, playing games, accessing apps, chat rooms, and any other access to the digital world via mobile phones, computers, tablets, gaming consoles, smart watches and any other device providing an access point to the world wide web.

1.2. The internet is largely an open unmanaged communication channel, which provides children and young people access to everyone who uses it and everything that is posted, with most of the content on the internet targeting adults it is largely unsuitable for children and young people.

1.3. Ofsted describe E-Safety as the "…ability to protect and educate pupils and staff on their use of technology" and we believe that education is key to providing support that children and young people need to keep themselves safe online, in whichever way that may be.

1.4. Children and young people may expose themselves to danger, knowingly or unknowingly when using digital technology via text messaging, phone calls, emails, chat rooms, instant messaging, websites, and social media. This is not exhaustive, but can lead to bullying and other types of abuse including:

- Radicalisation of extremist views.
- Sharing or exposure to inappropriate material that may cause distress.
- Contact with people who may groom or manipulate them into talking or acting provocatively or in a sexual way.
- Sexting, by sending or exchanging sexually explicit photographs or messages.
- Contact with people who may wish to exploit them for criminal activities.
- Threats and intimidation, prank calls, circulation of humiliating video's or information, and hate messages.
- Harassment or stalking, with repeated, prolonged, unwanted contact, or monitoring of another person.
- Prejudice-based bullying.
- Excluding individuals by setting up closed groups and refusing to acknowledge one user on purpose.
- Identity theft and hacking by finding out or guessing a user name and password.
- Trolling – a provocative email or posting intending to incite an angry response.
- Cyber-baiting, an example of this is inciting someone to lose his or her temper while filming it on a mobile phone. This video might then be uploaded to the internet.
- Fraping, a compound on Facebook and rape, describing someone's social networking profile being hacked into and changed.
- Ratting, a remote access Trojan (RAT) is a malware program that allows administrative control over the target computer.
- Click jacking – this is a malicious technique used to trick the user into clicking on something different from what the user thinks they are clicking onto. This might make the user vulnerable to giving confidential information and remotely taking control of their computer.

2. Statement of Principles:

2.1. As with all areas of life, the principles of keeping children and young people safe and protected in the digital world must be applied by parents/carers, professionals, and organisations that provide access to it, in this case Sydenham School.

2.2. Sydenham School has a responsibility to ensure students are safe online when in school, and that infrastructure must be in place to secure this legal responsibility.
2.3. While young people may be in a relatively secure environment while in school, this is not always the case at home or other locations.
2.4. Sydenham School has a vital role to play in fostering internet literacy. Parents often underestimate the experiences their children are exposed to.
2.5. The risk to young people is growing, this risk changes rapidly and is likely to affect the more vulnerable in the school community.
2.6. As with the real world, laws and legislation apply to safeguard and protect children and young people as the same exposure to exploitation and abuse exist. It is the responsibility of the e-safety champion to keep their knowledge of changes in the law up to date (including knowledge of the legislation and guidance on page 6 of the Lewisham Safeguarding Children Board's E Safety Guidance. file:///H:/DHT/E%20Safety/lscb_e-safety_guidance_june_2017.pdf

3. Definition:

3.1 The schools ICT system referred to in this policy encompasses all hardware, software, devices, communications and data that is owned by Sydenham School or connected to the Sydenham School network. This includes all data files that are stored in student and staff work areas which are by definition owned by the school.

3.2 The E-Safety Policy covers all use of these mediums both inside and outside school (via remote access), but also covers the use of specific knowledge gained as a result of being a member of the school community to publish to websites or other communications media outside school, e.g. on Social Networking Profiles or other digital collaborations. The Policy also covers the use of facilities provided by external organisations when undertaking school trips or visits, and all personal or other technologies used on the school site.

4. Policy Aims:

4.1. Policy Aim 1: To ensure students understand their responsibilities as digital citizens (both in and out of school), so that they are able to manage their online reputation and use ICT in safe and responsible ways

4.2. All users must be active participants in e-safety and digital citizenship education, taking personal responsibility for their awareness of the opportunities and risks posed by new technologies.

4.3. Sydenham School recognises the importance of educating our young people on how to stay safe online, and is committed to providing a stimulating curriculum to deliver e-safety and digital citizenship through Computing, PSHE and Citizenship lessons, as well as across the curriculum. All school staff should model safe and appropriate practices across the curriculum whenever technologies are used.

4.4. All teaching staff at Sydenham School receive annual safeguarding training which includes e-safety, and are committed to supporting every student in providing opportunities to use ICTs in a safe and responsible manner. We are also committed to providing regular opportunities to help staff consider their own safe use of ICT and the implications of its use.

4.5. Policy Aim 2: To ensure parents understand their responsibilities in modelling and promoting digital citizenship in the home, and how they can help to keep their children safe from harm

4.6. We also recognise the importance of providing advice and guidance to parents and carers and how to encourage safe use of the Internet and other technologies in the home, and regularly publish such materials through the school website, newsletter and at various events, including parents evenings. Full details on the responsibilities of parents can be found in the roles and responsibilities section of this policy.

4.7. Policy Aim 3: To ensure all staff are aware of their responsibilities in relation to e-safety and electronic communication and understand the school's approach to monitoring the appropriate (and inappropriate) use of ICT and outline sanctions for misuse;

4.8. All staff have a responsibility to educate students about e-safety where appropriate and to follow the Sydenham School Code of Practice for Electronic Communications (Appendix A). Full details on the responsibilities of staff in different positions within the schools can be found in the roles and responsibilities section of this policy.

4.9. **Policy Aim 4: To ensure all students understand the school's approach to monitoring the appropriate (and inappropriate) use of ICT and outline sanctions for misuse**;

4.10. All students are required to abide by the Rules for Acceptable Internet Use for Students which outlines the responsibilities of students when using ICT and the sanctions that can occur as a result of misuse (Appendix B). Full details on the responsibilities of parents can be found in the roles and responsibilities section of this policy.

4.11. Policy Aim 5: To ensure that the school has an effective and proportionate e-safety infrastructure in place, including effective monitoring and filtering technology.

4.12. It is the responsibility of the Network Manager to ensure that we have appropriate filters and monitoring systems in place and regularly reviewed. Whilst considering their responsibility to safeguard and promote the welfare of children, and provide them with a safe environment in which to learn, decisions about the effective use of filtering and monitoring technology should consider the age range of their pupils, the number of pupils, how often they access the IT system and the proportionality of costs vs risks. It should also be informed the risk assessment required by the Prevent Duty and be based on guidance by the UK Safer Internet Centre has published guidance as to what "appropriate" might look like: https://www.saferinternet.org.uk/advice-centre/teachers-and-professionals/appropriate-filtering-andmonitoring

4.13. Whilst ensuring e-safety, the Network Manager should be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding.

4.14. The Network Manager must ensure that these filters and monitoring systems can be used by Sixth Form students using mobile technology within the school and staff using school ICT off-site.

4.15. Virus protection software is installed and updated weekly by the Network Manager.

4.16. Policy Aim 6: To ensure that the school has a rigorous approach to auditing our approach to e-safety and that this is linked to governance;

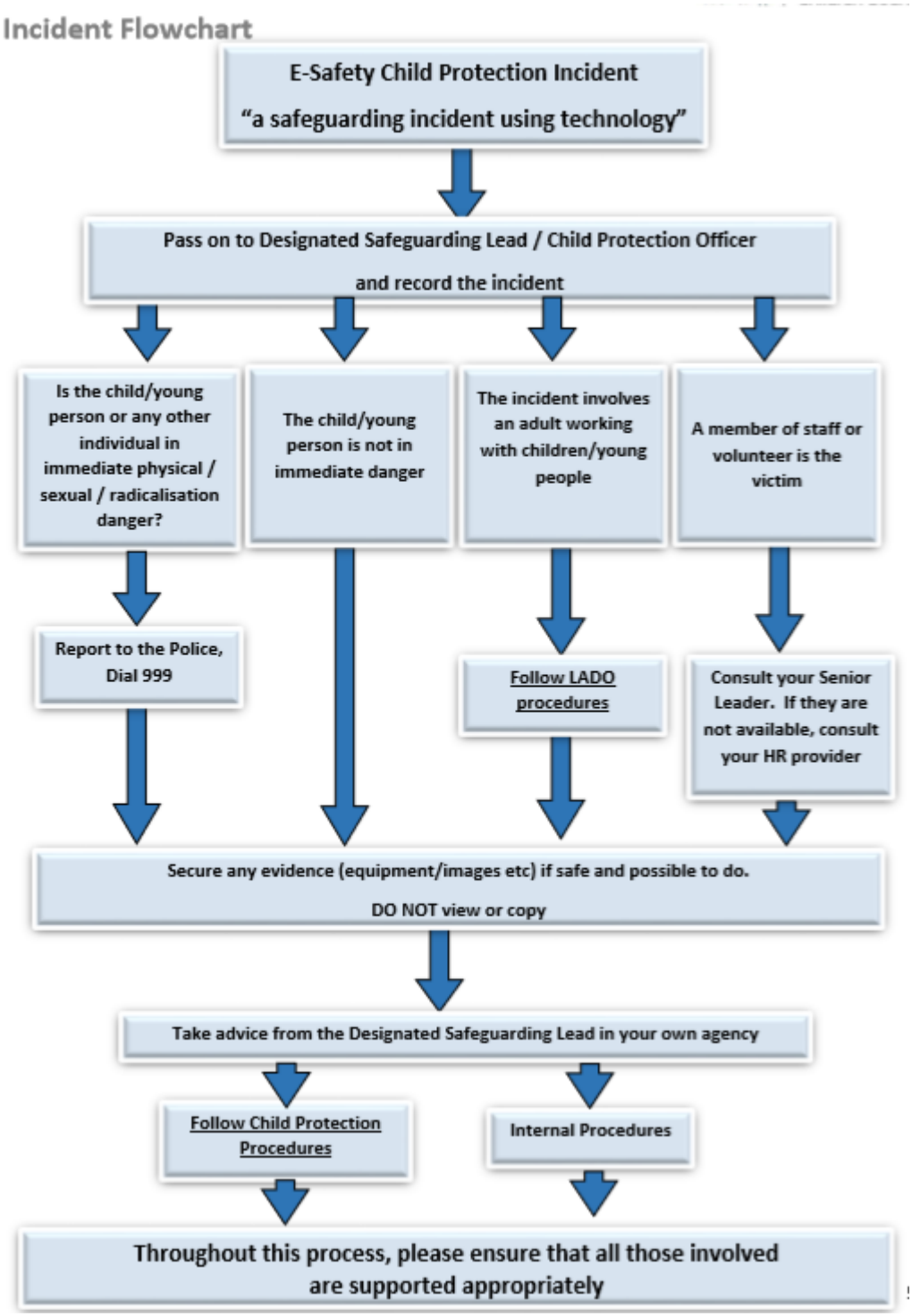
4.17. The E-Safety Champion is responsible for annually auditing the school's approach to e-safety and reporting to the Senior Leadership Team and the Governing Body, via the link E-Safety

Governor. The E-Safety Champion should do so using the exemplar template outlined in the LSCB E Safety Guidance. Lewisham Safeguarding Children Board's E Safety Guidance file:///H:/DHT/E%20Safety/lscb_e-safety_guidance_june_2017.pdf. To support this work, the E Safety Champion, or an appropriate other member of staff where this needs to be delegated, should attend the LSCB E-Safety Forum. https://www.safeguardinglewisham.org.uk/

4.18. It is the responsibility of the E-Safety Champion to ensure that actions identified in the E-Safety Audit are quickly implemented with regular reports provided to the school's Senior Leadership Team and Governing Body.

4.19. Policy Aim 7: To ensure that there is a consistent approach to incident management in relation to safeguarding incidents related to e-safety.

4.20. It is vital that all safeguarding incidents related to e-safety are dealt with in compliance with the Sydenham School Safeguarding and Child Protection Policy and the . In such incidents, there should be appropriate management of any e-evidence using the LCSB E-Safety Incident Flowchart. file:///H:/DHT/E%20Safety/lscb_e-safety_guidance_june_2017.pdf



5. ROLES AND RESPONSIBILITIES

5.1 The Role of Governors

1. Ensure the role of E-Safety champion is undertaken by an appropriate member of staff
2. Appoint an E-Safety governor who signs off an annual E-Safety audit and has an overview of all matters of digital citizenship and e-safety policy.
3. Ensure appropriate training is completed;

4. Ensure ICT usage is monitored appropriately within School and that agreed protocols are being followed in order to respond to e-safety incidents;
5. Ensure this policy is reviewed within the statutory timeframe by key staff and students;

5.2 The Role of Students

Students at Sydenham School are expected to:

1. Contribute to the development and review of the E-Safety Policy and related policies through the Student Council;

2. Read, understand and agree to the Acceptable Use Agreement and related policies and accepting the agreement at each logon;

3. Adhere to the E-Safety Policy and related policies;

4. Commit to growing and developing their ICT practice, through active involvement in the computing and citizenship and PSHE curriculum;

5. Take responsibility for keeping themselves – and others – safe online;

6. Take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies;

7. Assess the personal risks of using any particular technology, and behave safely and responsibly to limit those risks;

8. Respect the feelings, rights, values and intellectual property of others;

9. Seek help from a trusted adult if things go wrong, and support others who may be experiencing e-safety issues;

10. Follow the school's mobile phone policy at all times.

5.3 The Role of Staff

All staff delivering learning or care at Sydenham School have an essential role in creating an e- safe culture. The key responsibilities for all staff are:

1. Contribute to the development of the E-Safety Policy and related policies;
2. Read and adhere to the Acceptable Use Agreement and related policies, and accepting the agreement at each logon
3. Have an awareness of e-safety issues and how they relate to the children in their care;
4. Follow the school Safeguarding and Child Protection Policy in relation to safeguarding concerns related to e-safety.
5. To follow the procedures outlined in the LCSB E-Safety Incident Flowchart in the case of an e-safety incident. file:///H:/DHT/E%20Safety/lscb_e-safety_guidance_june_2017.pdf
6. Model good practice in using new and emerging technologies, emphasising positive learning opportunities;
7. Embed e-safety education in curriculum delivery wherever possible;
8. Remind students of school rules and procedures as required;
9. Monitor student use of the internet and other ICTs within the classroom, and take appropriate action as required;

10. Know when and how to escalate e-safety issues;
11. Maintain a professional level of conduct in their personal use of technology both within and outside school;
12. Take personal responsibility for their own professional development in this area;

5.4 The Role of the Senior Leadership team

The Senior Leadership team has statutory responsibilities for child protection and safeguarding, of which e-safety is an aspect. The key responsibilities of the Senior Leadership team are:

1. Ensure the role of E-Safety champion is undertaken by an appropriate member of staff.
2. Develop, own and promote the e-safety vision to all stakeholders;
3. Develop and publicise the strategy for the implementation and sustainability of e-safety, making appropriate resources available to support the development of an e-safe culture;
4. Support the Designated Safeguarding Lead and Deputy Designated Safeguarding Lead in the development of an e-safe culture;
5. Support members of staff in the appropriate escalation of e-safety incidents; 6. Take ultimate responsibility for e-safety incidents;
6. Report serious e-safety incidents to the governing body;

5.5 The E-Safety Champion

The key responsibilities of this role are:

1. Develop an e-safe culture under the direction of the Headteacher and act as the named point of contact on all e-safety issues;
2. Lead on the development of e-safety with input from all stakeholder groups;
3. Promote the e-safety vision to all stakeholders and support them in their understanding of the issues;
4. Ensure that e-safety is embedded within continuing professional development for staff and co-ordinate training as appropriate;
5. Ensure that e-safety is embedded across the curriculum as appropriate;
6. Ensure that e-safety is promoted to parents and carers, and other users of networked resources;
7. Maintain an e-safety incident log;
8. Monitor and report on e-safety issues to the Senior Leadership team and other agencies as appropriate;
9. Develop an understanding of the relevant legislation;
10. Liaise with the local authority or other bodies as appropriate;
11. Review and update e-safety policies and procedures on a regular basis;
12. Audit e-safety on an annual basis and report to the governing body.
13. Be the key link for the E-Safety Governor.
14. Know what to do if a child has knowingly or unknowingly acted inappropriately online.
15. Know what to do if an adult has knowingly or unknowingly acted inappropriately online.
16. Know how to make a referral to the Lewisham Local Authority Designated Officer (LADO) when an adult working with children and young people behaves inappropriately at the venue or online.

17. As part of the requirement of safeguarding children, ensure all staff undergo regular E-Safety training to understand the principles of keeping children safe whilst online and know how to respond to situations.
18. Advertise and promote safe use of equipment, games, applications, etc. on the internet.
19. Encourage parents to complete the LSCB E-Safety for Parents Course. http://www.safeguardinglewisham.org.uk/lscb/lscb/parents-carers/staying-safe-on-line
20. Attend the LSCB E-Safety Forum

5.6 The Role of the Network Manager and ICT Support Team

The key responsibilities for this team are:

- Support the E-Safety Champion in the development and implementation of appropriate e-safety policies and procedures;
- Provide a technical infrastructure to support e-safe practices, while ensuring that learning opportunities are still maximised;
- Take responsibility for the security of systems and data;
- Report any technical breaches to the E-Safety Champion and Designated Safeguarding Lead and take appropriate action as advised;
- Develop an understanding of the relevant legislation as it relates to the technical infrastructure;
- Liaise with the local authority and other bodies as appropriate on technical infrastructure issues;
- Read and adhere to all policies covered in the E-Safety Policy, including those in the appendix.
- Maintain a professional level of conduct in their personal use of technology both within and outside school;
- Take personal responsibility for their own professional development in this area;

5.7 The Role of Parents and Carers

The key responsibilities of parents and carers are:

- Contribute to the development of the E-Safety Policy and related policies through the Parent Forum; Read the Acceptable Use of ICT and E-Safety Policy and related policies, encourage their children to adhere to them, and adhere to them themselves when appropriate;
- Use technologies provided by the school for parental access safely and appropriately;
- Discuss e-safety issues with their children and support the school in its e-safety approaches by re-enforcing appropriate behaviours at home;
- Take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies;
- Model appropriate use of new and emerging technologies;
- Liaise with the school if they suspect, or have identified, that their child is conducting risky behaviour online
- Support the school and police with the effective management of e-evidence when on personal devices of students or parents.
- Consistently support the school in the implementation of the Mobile Phone Policy.

Appendix A: SYDENHAM SCHOOL STUDENT CODE OF PRACTICE FOR ELECTRONIC COMMUNICATIONS (Updated May 2018)

Introduction

1. Access to phones, e-mail and the Internet is provided to support the School in the provision and improvement of its services.

2. The School wants to create a learning environment for its staff and encourages all employees to become proficient in the use of e-technology. This will lead not only to new and exciting ways of service delivery but to a more enjoyable working environment for staff who can develop useful transferable skills. Staff are encouraged to become familiar with e-technology so that they can use it without difficulty.

3. Set out below is a Code of Practice regarding use of the internet, e-mail and phones. It provides a framework for operating within a rapidly changing area of activity. It is meant to enable all users to get the maximum benefit from those facilities. It clarifies the school's expectations of those using School telecommunications systems and identifies their responsibilities. Staff must comply with it.

4. In this document the term 'users' includes all School staff and any others authorised to use the School's telecommunications facilities in the course of their employment or provision of services to the School.

5. In particular, the school is committed to maximising appropriate email and Internet usage for the benefit of learning and encourages all users to be proficient in their use and to explore the possibilities that the internet and e-mail provide for service innovation. Using the Email and Internet offers great opportunities to work smarter and to improve services. The School wants users to make full appropriate use of these facilities.

6. E-mail and Internet access also introduce risks for the school as an organisation and for users as individuals. Many of these risks exist in other ways of working and communicating whether this is by letter, by telephone or in person. However e-mail and the Internet - and the way we use them - raise some particular issues. This document is an attempt to manage those risks constructively whilst promoting internet and e-mail use. It also provides guidance on authorised telephone use.

7. Personal devices should not be used to access the schools Email or network unless they are using the schools approved remote access portal. (Using the standard phone email client is not encrypted and therefore not GDPR compliant).

8. The Code of Practice may be supplemented from time to time by supplementary guidance that addresses the special circumstances that arise in some work areas. That supplementary guidance will apply in conjunction with this general Code of Practice and users must comply with both

9. Managers should also ensure that consideration is given to any special local considerations that require supplementary advice to people working in their work area. For example, where particularly sensitive data is handled on a day to day basis, or where best practice promoted by professional institutions is available, special attention may be required.

10. Use for School E-mail, internet and telephone facilities is provided only for School purposes. They should be used for that purpose. However, the School acknowledges that there may be occasional minimal use other than for School purposes. Examples of excessive use would include; single use involving several hours during working time and/or repeated episodes of shorter use during working time. These examples are not exhaustive.

11. Personal use. Some uses are absolutely forbidden (such as accessing pornographic sites on the Internet or using e-mail to forward pornographic images). In other circumstances, what is acceptable is a matter of degree. If in doubt users should seek advice from their manager.

12. Infrequent minor use of telephone, e-mail and the internet for personal purposes may be permissible if the following criteria are observed:- ·

- The use of internet or e-mail is outside the School's core hours
- The use is not for a purpose which is prohibited by this code of practice or explicit management instruction
- Personal use by the user is not excessive, whether on a single occasion or in general.
- The personal use does not detract from the user's ability to perform their duties properly, or that of their colleagues.
- The use is not in contravention of this Code of Practice
- The privilege of personal use has not been withdrawn either generally or from the individual by a manager. Managers may not consent to use of the facilities other than in accordance with this paragraph.

Because of the cost of mobile telephone calls, employees who use them for personal use are required to reimburse the costs incurred in such use.

Personal use of telephones, e-mail and access to the Internet, like any School facility is a privilege, which may be withdrawn at any time and users must justify their use of internet and e-mail if asked to do so.

13. Prohibited Use of Internet and E-mail Users may not use the School's phones, or computer systems including e-mail and internet facilities for any of the following:

- any criminal activity,
- gambling,
- creating, accessing, distributing, storing or downloading - pornographic material - material that is racially or sexually or otherwise offensive
- to distribute defamatory material of any kind
- party political purposes
- harassment of any person
- use of 'chat room' communities on the Internet other than in connection with School business
- downloading games, screen savers or other executable programs
- distributing 'chain mail'
- any other purpose which the School informs employees is a prohibited use

Managers may not consent to use of phone, internet or e-mail for any of these purposes.

Monitoring

14. The School routinely and randomly monitors accessed internet sites and e-mail on its computers as well as the extent of telephone usage.

15. The School reserves the right to monitor telephone calls, internet sites accessed or e-mail sent or received using its facilities for the purposes of detecting unauthorised use, fraudulent or other criminal activity and improving service provision. Users should be aware that the School may monitor use of all telecommunications facilities. Therefore management checks on use of these

facilities may mean that others have access to any messages sent on School facilities. There can be no expectation of privacy in anything created, accessed, stored, sent or received on the School's telecommunications and computer systems.

16. You must take as much care with communication by e-mail as with any other written form of communication. E-mail is routinely stored, can be misdirected very easily and cannot be retrieved as some other forms of written communication can be. There are particular risks with personal use of e mail where your language may be less formal and particular risks with e-mail that is being sent externally since this can be interpreted as committing the school in a way that was not your intention.

17. Sending, receiving and holding e-mail correspondence may involve the processing of personal data which must be dealt with in accordance with the GDPR 2016 (General Data Protection Regulations). This may require you to notify and/ or seek the consent of the subject about why you are processing their personal data and who you may pass it to. They may also be entitled to a copy.

18. E-mail is generally not a secure method of communication, although encrypting messages can provide some security. As a general rule, e-mail should not be sent that includes sensitive information that can be associated with individuals.

Inappropriate use

19. Defamation: In all forms of communication if you make negative statements about a person or another business based on false statements of fact you run the risk of being sued for libel or slander and exposing the school to potential liability. E-mail and other electronic communications (bulletin boards etc) pose a particular threat of claims for defamation because of the speed with which e-mail can be created and sent, and because on-line information can be distributed more widely. Users must not use defamatory language in any communication

20. Bullying/ harassment: Given the speed with which electronic communication can be created and sent there is a risk that poorly written and/ or repetitive communication will be taken as bullying or harassing colleagues. This is no more acceptable electronically than in any other form.

21. Pornography: There is no legitimate business interest in employees accessing or transmitting sexually explicit material while at work. Nor is it acceptable to the School that anyone should use School facilities for creating, accessing or transmitting such material for personal use. You must not do so and you must report any accidental access to such sites or telephone numbers.

22. Overall, material that is fraudulent, harassing, embarrassing, sexually explicit, profane, obscene, intimidating, defamatory, or otherwise unlawful or inappropriate must not be sent by phone, e-mail or other form of electronic communication, or displayed on or stored in School computers. Users encountering this type of material by accident or receiving it must immediately report the incident

23. School telecommunications and computer systems may not be used for personal business use. This includes the dissemination or storage of commercial or personal advertisements, solicitations or promotions.

24. Gambling: Lewisham's telecommunications and computer systems may not be used for gambling.

Access

25. You may not alter or copy a file belonging to another user without their permission and you may not use the computer system to unnecessarily view other people's files or e-mail. You should not access or attempt to gain access to any restricted computer files. Nor should you seek to circumvent data protection measures that are installed on the system.

Protecting school property

26. Passwords are the principal means by which access to your computer and your documents is controlled. You must take care not to disclose your password to anyone. You should change your password if it becomes known to anyone else and otherwise at least every 60 days.

27. You must take precautions against introducing viruses to the school's computer systems. You must only access the Internet through a computer attached to the school's network through the firewall. You should not access the Internet directly.

28. You should not install or use unauthorised encryption software. There are laws on the export of encryption software

29. You must never seek to mask your identity in anyway when using e-mail.

Copyright

30. The risk of copyright infringement is greater using e-mail than traditional communication methods and there are particular risks associated with forwarding copies of e-mails. You do not 'own' material just because it has been sent to you. You must ensure that you are not breaking copyright law in sending material by email.

31. Much of the software on the school's computers is governed by licence agreements. These licences do not generally allow for software to be copied and you must not copy any software for use on home or other computers.

Use of resources

32. You must not deliberately perform acts that waste computer resources or unfairly monopolise resources to the exclusion of others. These acts include sending mass mailings. Chain e-mail (a message sent to a number of people asking each recipient to send copies with the same request to a specified number of others) can quickly become a substantial drain on computer resources. In turn, this can reduce the effectiveness and the speed of your computer. You must not distribute chain e-mail.

33. You should not store unnecessary copies of e-mail correspondence, although you should consider whether material should be kept. If you are in doubt about whether correspondence should be retained, please consult your line manager. 34. You should not use unencrypted storage media for any data or document that contains any personal data that could identify any individual (student or staff). Any storage or use of data or information is regulated under the GDPR 2016.

Breach of Code of Practice

35. Breach of this Code of Practice will be taken seriously and may result in disciplinary action, including possible dismissal without notice or warning, and/or civil and/or criminal liability and/or withdrawal of the facilities. If you are unsure about any issue concerning use of e-mail or the Internet ask! In normal circumstances, raise the issue with your line manager in the first instance.

36. In particular breaches of paragraphs 9 and 10 of this Code of Practice may potentially be deemed to be gross misconduct and may result in dismissal. However, this is not meant to be exhaustive.

Appendix B: RULES FOR ACCEPTABLE INTERNET USE FOR STUDENTS.

Only access the Internet if your parents/guardians have given their permission.

Ask permission from a teacher before accessing the Internet.

Only use the Internet when there is a teacher present.

Always ask permission from a teacher before downloading anything, or printing anything whether information, graphics or software.

Only use the Internet for research or school purposes.

Only use your own password, do not use anyone else's.

Remember that not everything you see online is accurate or true.

Always quote the source of any information, data, graphics, images etc from the Internet i.e. the web address, in the work you produce.

Whenever possible, know who created the web site you are about to access.

Never send or display offensive messages or pictures.

Do not violate copyright laws.

Do not waste time on the Internet.

Do not view, keep or send anything that you would not want your parents/ guardians or teachers to see.

Always tell a teacher if you see bad language or distasteful pictures while you are online.

Never respond to unpleasant, rude or suggestive e-mails or postings.

Do not access chatrooms and should you meet anyone on the Internet never send them your picture, home address or telephone number.

Never arrange to meet anyone in person through the Internet. Remember that some people online may not be who they seem.

Never cause damage to the system.

SANCTIONS:

At Sydenham we have the ability to monitor all computer activity at any time, including seeing all communications as they happen. Further, all sites accessed are logged against user names, and staff regularly review all Internet usage.

Violation of the above rules will automatically result in the suspension of Internet use either short term or permanently. Parents may also be informed.

Additional disciplinary action may be taken if there are violations of the schools Behaviour Policy or our Equal Opportunities Statement.