The Billericay School

E-Safety Policy

Date of Last Review:	Jan 2021
Status:	Statutory
Committee:	TBC
Staff Lead:	Charlotte Berry
Review Process:	Annually
Location:	R:\SLT\Policies
Date of Next Review:	Sept 2022

INDEX

SECTION 1

INTRODUCTION

INTRODUCTION

ICT in the 21st Century is 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. The school recognises this and the role we have to play in ensuring our students gain the ICT skills necessary for everyday life, life-long learning and employment.

We also recognise, however, that the use of technologies presents risks as well as benefits; new technologies, particularly web-based resources, are not consistently policed and bring students into contact with a wide variety of influences, some of which may be unsuitable or harmful. Unmediated Internet access through computers, telephones, iPads etc. brings with it the possibility of placing students in embarrassing, inappropriate and even dangerous situations. 'Keeping Children Safe in Education' identifies the following three areas of e-safety risk in relation to students:

- *Content: Being exposed to illegal, inappropriate or harmful material*
- *Contact: Being subjected to harmful online interaction with other users*
- *Conduct: Personal online behaviour that increases the likelihood of, or causes, harm*

The school takes seriously its responsibility to ensure that students are able to use internet based resources safely in school and are equipped, through the curriculum, to use the internet and social media safely and legally at all times.

The school also recognises that we hold personal data on students, staff and others that we use to conduct our day-to day activities, and that some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. Everyone at Billericay School has a shared responsibility to secure any information used in the course of their professional duties and we undertake training of all staff to ensure they are aware of the risks and threats, and how to minimise them.

CORE PRINCIPLES

Responsibility:

- All teaching staff, support staff, supply staff, governors, visitors, external contractors, volunteers and other individuals who work for or provide services to the school (referred to collectively as staff), as well as children and parents/carers have a responsibility to abide by the terms of this policy.

- All curriculum internet use will be planned, task-orientated and educational and undertaken in a regulated and managed environment.

Scope:

- This policy applies the use of all information communication/internet enabled devices, including in-school equipment, personal devices brought onto the school site and any school devices used for off-site access.

- This policy should be read in conjunction with other relevant school policies including (but not limited to) Safeguarding & Child Protection Policy, Anti-Bullying Policy, Behaviour Policy, Code of Conduct & Whistleblowing Policy, Acceptable Computer & Internet Use Policy, Data Protection Policy, PD Policy, Home School Agreement.

- The policy has been approved and agreed by the Senior Leadership Team and the Governing Body.

- The school has appointed a member of the Governing Body to take lead responsibility for e-Safety.

- The school has appointed a member of the Senior Leadership Team as the E-Safety Lead and Team (Mrs C. Berry).

- The school's E-Safety Policy and its implementation will be reviewed at least annually or sooner if required.

Legislation:

- This policy incorporates guidance contained in 'Keeping Children Safe in Education: Statutory Guidance for Schools & Colleges (2019) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/811513/DRAFT_Keeping_children_safe_in_education_2019.pdf

- It recognises advice contained in 'The Prevent Duty: Departmental Advice for Schools & childcare Providers (2015) https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/439598/prevent-duty-departmental-advice-v6.pdf

- It recognises advice contained in 'Sexting in Schools & Colleges: Responding to Incidents and Safeguarding Young People https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/551575/6.2439_KG_NCA_Sexting_in_Schools_WEB__1_.PDF

AIMS

- To ensure that online safety (e-safety) is seen as an essential element of safeguarding children and adults in the digital world, and that all steps possible are taken to enable our students and staff to use technology such as computers, mobile phones, games consoles or other internet enabled devices in as safe and risk-free way as possible.

- To provide a curriculum and in-school environment that teaches and supports our students to manage and respond to risk, and empowers them to build resilience online.

- To provide the school community with quality Internet access to raise education standards, promote student achievement, support the professional work of staff and enhance the school's management functions.

- To ensure the internet provision in school is monitored and provides safe access for all users.

OBJECTIVES

- To identify the key principles expected of all members of the community with regards to the safe and responsible use technology to ensure that the school is a safe and secure environment.

- To safeguard and protect all members of the school's community online.

- To raise awareness of the potential risks, as well as benefits, of technology with all members of the school's community.

- To enable all staff to work safely and responsibly, to role model positive behaviour online and be aware of the need to manage their own standards and practice when using technology.

- To identify clear procedures to use when responding to online safety concerns that are known by all members of the community.

SECTION 2

RESPONSIBILTIES

KEY RESPONSIBILITIES OF THE SENIOR LEADERSHIP TEAM

- To develop and promote the e-safety vision and culture to all stakeholders in line with national and local best practice recommendations with appropriate support and consultation throughout the school community.
- To audit and evaluate current e-safety practice to identify strengths and areas for improvement.
- To support the E-Safety Lead and Team in the development of an online safety culture within the school.
- To ensure there are appropriate and up-to-date policies and procedures regarding online safety.
- To ensure that suitable, age-appropriate and relevant filtering is in place to protect students from inappropriate content (including extremist material) to meet the needs of the school community and ensuring that the filtering and school network system is actively monitored.
- To ensure all members of staff receive regular, up-to-date and appropriate training regarding e-safety roles and responsibilities and provide guidance regarding safe appropriate communications.
- To ensure that online safety is embedded within a whole school curriculum that enables all students to develop an age-appropriate understanding of online safety and the associated risks and safe behaviours.
- To make appropriate resources available to support the development of an e-safety culture.
- To take responsibility for online safety incidents and liaising with external agencies as appropriate.
- To review online safety incident logs and use them to inform and shape future practice.
- To ensure there are robust reporting channels for the school community to access regarding online safety concerns, including internal, local and national support.
- To ensure that appropriate risk assessments are undertaken regarding the safe use of technology, including ensuring the safe and responsible use of devices.
- To work with and support technical staff in monitoring the safety and security of the school's systems and networks.
- To ensure a member of the Governing Body is identified with a lead responsibility for supporting e-safety.

KEY RESPONSIBILITIES OF THE DESIGNATED E-SAFETY LEAD AND TEAM

- To act as a named point of contact on all e-safety issues and liaising with other members of staff and agencies as appropriate.
- To keep up-to-date with current research, legislation and trends.

- To co-ordinate participation in local and national events to promote positive online behaviour, e.g. Safer Internet Day.
- To ensure that e-safety is promoted to parents and carers and the wider community through a variety of channels and approaches.
- To ensure that all data practices are in-line with legislation.
- To maintain an online safety incident/action log to record incidents and actions taken as part of the schools safeguarding recording structures and mechanisms. This will be in the safeguarding and child protection folders. Internet and network bans will be kept within the SIMS as a clear indication of incidents over the past years.
- To monitor the school's e-safety incidents to identify gaps/trends and update the education response to reflect need.
- To review and update the E-Safety Policy, Acceptable Computer & Internet Use Policy and other procedures on a regular basis (at least annually) with stakeholder input.
- To ensure that online safety is integrated with other appropriate school policies and procedures.

KEY RESPONSIBILITIES OF STAFF

- To adhere to the school's Acceptable Computer & Internet Use Policy.
- To take responsibility for the security of school/ systems and data.
- To have an awareness of e-safety issues, and how they relate to the students in their care.
- To model good practice in using new and emerging technologies.
- To embed e-safety education in curriculum delivery wherever possible.
- To identifying individuals of concern, and taking appropriate action by working with the E – Safety Lead.
- To know when and how to escalate e-safety issues, internally and externally.
- To be able to signpost to appropriate support available for e-safety issues, internally and externally.
- To maintain a professional level of conduct in their personal use of technology, both on and off site.
- To take personal responsibility for professional development in this area.

ADDITIONAL RESPONSIBILITIES FOR STAFF MANAGING THE TECHNICAL ENVIRONMENT

- To provide a safe and secure technical infrastructure which supports safe online practices while ensuring that learning opportunities are still maximised.
- To take responsibility for the implementation of safe security of systems and data in partnership with the leadership and management teams.
- To ensure that suitable access controls and encryption is implemented to protect personal and sensitive information held on school-owned devices.

- To ensure that the school's filtering policy is applied and updated on a regular basis and that responsibility for its implementation is shared with the E-Safety Lead and Team and Designated Safeguarding Lead.
- To ensure that use of the school's network is regularly monitored in order that any deliberate or accidental misuse can be reported to the E-Safety Lead and Team.
- To report any breaches or concerns to BYC or other member of SLT (or HOH if appropriate) depending on the nature of the incident and together ensure that they are recorded on the e-safety Incident Log, and appropriate action is taken as advised. IT Technical staff may be asked for support to gather evidence.
- To develop an understanding of the relevant legislation as it relates to the security and safety of the technical infrastructure.
- To provide technical support and perspective to the E-Safety Lead and Team and SLT, especially in the development and implementation of appropriate e-safety policies and procedures.
- To ensure that the school's ICT infrastructure/system is secure and not open to misuse or malicious attack.
- To ensure that appropriate anti-virus software and system updates are installed and maintained on all setting machines and portable devices.
- To ensure that appropriately strong passwords are applied and enforced.

KEY RESPONSIBILITIES OF STUDENTS

- To read the school's 'Acceptable Computer & ICT Use Policy' and adhere to it.
- To respect the feelings and rights of others both on and offline.
- To seek help from a trusted adult if things go wrong, and supporting others that may be experiencing online safety issues.
- To take responsibility for keeping themselves and others safe online.
- To take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- To assess the personal risks of using any particular technology, and behave safely and responsibly to limit those risks.
- To support our 'no mobile phone use or internet enabled devices in school' policy

KEY RESPONSIBILITIES OF PARENTS AND CARERS

- To read the school's 'Acceptable Computer & ICT Use Policy' and encourage their children to adhere to it, and adhere to it themselves where appropriate.
- To discuss e-safety issues with their children, supporting the school in their e-safety approaches, and reinforce appropriate safe online behaviours at home.
- To role model safe and appropriate uses of new and emerging technology.
- To identify changes in behaviour that could indicate that their child is at risk of harm online.

- To seek help and support from the school, or other appropriate agencies, if they or their child encounters online problems or concerns.
- To use the school's systems, and other network resources, safely and appropriately. Parents are encouraged to use a filtered system and may use the schools system via the portal from home to ensure a high level of filtering for their children.
- To take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- To support our 'no mobile phone use or internet enabled devices in school' policy

SECTION 3

MANAGING INTERNET SAFETY

TECHNICAL & INFRASTRUCTURE APPROACHES

The school uses the following:

- An educational, filtered secure broadband connectivity through an industry standard internet filter that is exceptionally secure.
- The Palo filtering system that blocks sites that fall into categories such as pornography, race hate, gaming, sites of an illegal nature, etc. All changes to the filtering policy are logged and only available to staff with the approved 'web filtering management' status.
- USO (Unified sign on service) user-level filtering where relevant, thereby closing down or opening up options appropriate to the age / stage of the students.
- Sophos anti-virus software and an appropriate network set-up to ensure the network stays safe by preventing staff and students from downloading executable files.
- Individual, audited log-ins for all users.
- DfE, LA Microsoft 365 secured email to send personal data over the internet and encrypted devices and secure remote access where staff need to access personal level data off-site.
- Blocks on all chat rooms and social networking sites except those that are part of an educational network.
- Unblocks of other external social networking sites for specific purposes / internet literacy lessons.
- Only approved or checked webcam sites.
- Blocked access to music download for pupils.
- Security time-outs on internet access where practicable / useful.
- Highly restricted, safe e-mail and access to an educational Microsoft Account.
- Provision for staff of an email account for their professional use, and makes clear personal email should be through a separate account.
- Teacher 'remote' management control tools for controlling workstations, viewing users, setting-up applications and Internet web sites, where useful.
- Additional local network auditing software is installed through Impero which tracks user activity across a session.

- A network manager who is up-to-date with school services and policies and requires the service providers to be up-to-date with school services and policies.

SECTION 4

EDUCATING THE SCHOOL COMMUNITY

The Billericay School understand the importance of education and training in relation to e-safety. We provide all members of the school community with information, training and support that allows them to use the internet and social media confidently and safely, whilst also making them alert to the potential dangers.

STUDENTS

Students are taught how to use the internet and social media safely and responsibly.

The school's Computer Science curriculum includes schemes of work dedicated to e-safety. In Year 7 the students start the year by following a 12 week course that introduces them to the school network, looks at the 'Acceptable Computer & Internet Use Policy' and considers a variety of e-safety issues; the topics covered include social networking, cyber-bullying, phishing and viruses – students consider the safety issues related to each, what they can to avoid them and how to report any concerns or incidents. Year 8 and 9 students follow a 4 week course that looks at 'ICT in Society'. The unit revisits the topics of social networking and cyber-bullying as well as considering the impact of mobile technologies on society and the environment; students consider each aspect from social, economic, ethical and moral perspectives and how the behaviour of individuals affects others, as well as considering the safety issues, how to avoid them and what do if they encounter problems.

The school's Personal Development curriculum includes schemes of work in each of Years 7-11, which consider all aspects of e-safety. Year 7 look at 'Keeping safe on-line' and how to 'Use your smart phone smartly'. Year 8 focuses on cyber-bullying and this continues in Year 9, alongside issues and legislation related to 'Sexting' [Youth Produced Sexual Imagery]. In Year 10, the previous years' themes are developed to consider aspects including 'Child Sexual Exploitation' and 'Radicalisation', and the role the internet plays in these. Years 12 & 13 consider a range of e-safety themes as a part of the 6th Form Future Citizenship programme. Schemes of Work are reviewed and updated at least annually and in response to contextual safeguarding issues and local and national trends.

Assemblies are used as a vehicle to reinforce the topics and issues covered in the Personal Development Programme for Years 7-13 and, as such, all year groups receive e-safety presentations on a regular basis.

There is a dedicated 'E-Safety' area for our students on the school website http://www.billericay.essex.sch.uk/students/e-safety/. This includes the 'STOP & THINK before you CLICK' materials.

All curriculum areas take the opportunity to re-inforce the ‘e-safety’ and ‘safe internet use’ messages when using mobile or internet based resources within lessons.

Our over-arching aims in relation to the e-safety education and support we offer our students are to:

- Foster a ‘No Blame’ environment that encourages pupils to tell a teacher or responsible adult immediately if they encounter any material that makes them feel uncomfortable
- Ensure students know what to do if there is a cyber-bullying incident
- Ensure students know how to report any on-line abuse
- Have a clear, progressive e-safety education programme that runs from Year 7-13 and is built on national guidance
- Assist students to develop a range of strategies to validate and verify information before accepting its accuracy;
- To help them understand ‘Netiquette’ behaviour when using an online environment, social network, email or text/media messaging; this to include -being polite, not using bad or abusive language or other inappropriate behaviour; keeping personal information private
- To ensure students understand how photographs can be manipulated and how web content can attract the wrong sort of attention
- To ensure they understand why on-line ‘friends’ may not be who they say they are and to understand why they should be careful in online environments
- To ensure they understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings
- To ensure students understand why they must not post pictures or videos of others without their permission
- To be aware they may know not download any files – such as music files - without permission
- To support students to develop strategies for dealing with receipt of inappropriate materials
- To ensure students understand why and how some people will ‘groom’ young people for sexual reasons
- To place social media/e-safety guidance in student planners.

STAFF

Staff receive information on e-safety that ensures that they understand the safeguarding issues related to use of the internet both by their students and themselves, that they understand how best to use mobile devices and the internet safely, and they understand both the school's procedures and sanctions for dealing with internet or network abuse as well as the routes for reporting externally.

A planned & calendared programme of e-safety training opportunities is in place for staff; these are delivered via compulsory whole-staff training sessions and flexible training sessions that staff can opt to attend. In addition, key members of staff complete online training, external CPD courses and accredited CPD courses (for example, those run by CEOP – Child Exploitation and Online Protection Centre).

E-Safety information is also delivered directly to staff via e-mail, the school website and social media sites, staff bulletins or subscribed news e-mails.

All staff are made aware of, and asked to sign, the 'Acceptable Computer & Internet Use Policy' (see Appendix 1a) and sign to say they understand and accept the contents. New staff and trainees receive additional training in this area.

In addition, staff have access to a dedicated area of the school network where information leaflets and guidance are available; this includes, for example, 'A Staff Guide to Social Networking'. Staff also have access to the extensive e-safety resources available on our website.

Our over-arching aims in relation to the e-safety education and support we offer our staff are to:

- Ensure staff know how to respond if they find, or are made aware of, inappropriate use of the network, accessing of inappropriate internet sites or sending and receiving of inappropriate online materials
- Ensure staff know how to respond to issues of cyber-bullying, sexting or other on-line activity that is brought to their attention
- Ensure staff are aware of the 'Using Social Network Sites (SNS) in School' guidance and adhere to its principles
- Ensure staff feel confident in supporting our students to behave safely whilst online or using mobile devices
- Ensure staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection

GOVERNORS

Governors have access to e-safety training in a range of formats. The governing body can elect to receive e-safety training via their scheduled governor training sessions. They are also invited to attend key staff training sessions, have access to online and external CPD courses and are encouraged to follow guidance issued online via membership of bodies such as the 'National Governors Association'.

PARENTS & CARERS

Parents have e-safety information delivered to them directly via the school newsletter and links to external agencies such as ‘Parent Zone’ via the school website. The website has a dedicated area for parents, which contains a wide variety of information, guidance and support in relation to e-safety; topics include ‘cyber-bullying’, ‘sexting’, ‘A Guide to Facebook’.

The school also runs e-safety information sessions for parents as the need arises.

Parents receive, and are asked to sign, a copy of the school’s ‘Acceptable Computer & Internet Use Policy’ (see Appendix 1b).

SOCIAL NETWORKING GUIDE

Using Social Network Sites (SNS) with the School

Social Media provides a fantastic way of sharing information quickly and easily. Twitter and Facebook are an easy way to share information and news.

General Guidance

As long as parents/carers are in agreement and age restrictions are followed, students are able to use social networking sites in their own time. There are privacy options on most SNS to limit who can read posts and access other information – students should use these wisely. We are happy for students to 'follow' our official profiles on Twitter or a school Facebook page as appropriate:

- We will not 'follow', 'add' or 'like' any student in this school or known minor
- We will not 'follow' individuals unless there is an educational or community link
- We will not monitor what students post on SNS, although we may look at students' social media if issues relating to student safety and welfare are brought to our attention and the sites are public.
- Students and their parents/carers are responsible for what they post online and guidance and support is given in school via ICT, PD and the Pastoral Curricula.
- We may post pictures of events which include students as long as parents/carers have not withdrawn permission.
- We will closely monitor our accounts but they are not used as a channel of communication for students and/or parents/carers. Telephone, email or letter should remain the main method of contacting the school.
- We may take action/delete posts if someone posts something in the public domain which is unsuitable or offensive and is reported to us or sent directly to us or our page.

Advice for staff

Many teachers use social networking services (SNS), such as Facebook and Twitter, in order to stay in touch with friends and family. This guide is designed to support your personal use of these services, keeping you, your students, and your job safe. For more advice on e-safety see the school website and e-safety policy or speak to Mrs Berry, Deputy Headteacher.

KEY QUESTIONS

1: Can I be friends with my pupils on social networking services?

Do not accept friend requests on your personal account from pupils. You may be leaving yourself open to allegations of inappropriate contact or conduct or even find yourself exposed to unwanted contact. (On most services, the sender won't be notified if you select ignore/not now or delete for such requests, nor, if you had already accepted such a request, will they be notified if you remove them from your friends list or followers). **There is clear guidance supported by the Teaching Unions to say that friending pupils is not appropriate**. Be careful about accepting requests from friends who are former pupils or parents of pupils as by accepting such requests you could be making yourself vulnerable by sharing personal information or by having access to personal information about pupils. If you accept former pupils after they are 18 and not returning to year 14, be mindful of the fact they may have younger siblings/friends who are still at school.

2: Can I use sites like Facebook or Twitter in school for educational purposes with my pupils?

Social networking services are blocked for most of the school but with careful planning and management, they can be used responsibly by staff to communicate information (e.g Sixth Form Twitter; A level Media Tumblr) **A professional account or page must always be used and approval must first be sought from SLT**. Remember that most SNS do have a minimum age requirement of 13 and that we have a 'No Phone Use in School' Policy; young people actually need a break from the ever present mobile technology.

3: Which privacy settings do I need as a teacher if I am using social networking services?

The answer will depend on what you have on your profile, and what you tweet or post. You should never post anything which compromises your professional reputation. Do not write about colleagues or write updates about pupils. **Do not post pictures of pupils** whatever the context as this infringes their right to privacy. **It is important that when using SNS you are in control of who can see your account details and content** including photos and albums, posts, status updates and any personal information. On Twitter, you can set your account to private by selecting 'Protect my tweets' so you can then accept (or decline) requests to follow you. In the case of Facebook, choosing a basic "friends only" setting for every option would initially achieve this.

However, you are able to customise each option further, and can limit the information that certain individuals see. It is a good idea to use the 'preview my profile' option, to check and see how your profile appears to strangers, and that the information you want to remain private or 'friends only' is not visible. If you are unsure about how to use the settings available, treat all information that you post as being public and act accordingly.

Think carefully about whom you are friends with, and which friends can access what information. It is a good idea to remove any 'friends' or customize the privacy settings for current friends, if access to your personal activity could compromise your position, for example parents with children at your school. However, whatever setting you use, it's important always to think before you post because 'friends only' settings do not guarantee privacy. Sharing content with others could mean that you lose control of it, if friends pass on your information, for example. Think carefully about comments you post on friends' walls – if their profile is not set to private your posts will be visible to anyone.

4: How can I continue to protect my professional reputation?

Your professional reputation is clearly valuable to your current and future career and consequentially managing your online reputation is an essential part of being a teacher. Always think carefully before making any posts, status updates or having discussions regarding the school, its staff, pupils or parents in an online environment – even if your account is private. Comments made public could be taken out of context and could be very damaging. Think about the language you use – abrupt or inappropriate comments, even if they were made in jest, may lead to complaints. Anything that is put online is potentially public and permanent.

Posting derogatory comments about pupils, parents or colleagues is never acceptable. Teachers are required to uphold the reputation of the school, to maintain reasonable standards in their own behaviour, and to uphold public trust in their profession. Bringing your school or your profession into disrepute may cost you your job.

Use a strong password, and log out of the SNS after using it. Not logging out means the next user of the computer or other access point can access your SNS account. (Deleting cookies may be necessary if you had selected the 'remember this password' option when you were logging in). If you access social networking via an application on your mobile phone, it is a good idea to set a PIN or passcode for the phone, and to remember to log out of the SNS app after each session, so if you mislay your phone, access to your SNS account is still protected.

Be mindful of how you present yourself when you are choosing a profile image, for example, or even when joining a Group or 'liking' pages – think about what these choices say about you.

Consider making private, or removing, previous online content that might compromise your current position. It is possible to deactivate existing SNS accounts and to permanently delete profiles. It is important to be aware, however, that though such changes will be immediate on the service itself, content which was visible on public search may still be visible on public search results for a week or two (or even longer) until these changes have been recognised by the search engine.

Searching your name regularly on public search engines can be a useful way to monitor your online content or 'digital identity'. Other tools are also available, for example, utilising privacy settings and removing your profile page from a search engine result.

Your online reputation is important for your current and future employment – it is common for employers to search prospective employees online.

5: What should I do if I see or am told about inappropriate content on social networking sites about my pupils?

If you come across, or are made aware of, inappropriate use of social networking sites by your pupils (including under age use of these services), you should report these in the first instance to Mrs Manchee and the Head of House. If you are concerned that it is potentially a safeguarding issue then report directly to Mrs Cooper, Mrs Berry or Mrs Smears.

6: What should I do if other people post inappropriate images of me online? How about if I am the victim of cyberbullying?

If you are unhappy with photos in which you are tagged, untag yourself or alternatively contact the friend and ask them to remove this content. Never be shy about asking others to take down or make private content that identifies you that you are not comfortable with. Be thoughtful about content you post that relates to others, and respond positively to requests to take down or make content private. If you think that the image or video breaks the SNS's terms of use, report it to the SNS who can take content down (look for the Report Abuse options in the service).

If you are concerned that a pupil is contacting you inappropriately or posting about you on SNS, seek advice from Mrs Berry, Mr Berry or Mrs Cooper.

SECTION 5

MOBILE DEVICES

MOBILE PHONES

Students in Years 7-11 are not allowed to use mobile phones, or bring other internet enabled devices, into school.

If staff see or hear a student's mobile phone in school, it will be confiscated as follows:

- Mobile phones confiscated before the lunch break will be returned at 3.00 p.m. the same day.

- Mobile phones confiscated during or after lunch will be returned at 3.00 p.m. the following school day.

All confiscated mobile phones are taken to Student Services where they are logged and placed in a safe. They may be collected from Student Services at 3.00 p.m. as set out above. Students needing to contact a parent / carer can ask to use the school phone at Student Services or F block reception.

INVESTIGATIONS INVOLVING MOBILE PHONES

Children's safety when using mobile phones and other internet enabled devices is the responsibility of parents.

Parents should be aware of how their children are using their phones and social networks. We advise frank, open discussion so that parents are informed about what risks their children may be exposing themselves to in the digital world. There is also a wealth of advice and guidance for parents on the website: http://www.billericay.essex.sch.uk/parents/using-the-internet-and-smartphones-safely
We expect students and their parents to follow advice about age recommendations for different social network sites and apps: https://www.net-aware.org.uk/

We expect parents to have talked to their children about privacy settings and advise that students in KS3 or 4 have private accounts to which only close friends and family are allowed access.
We will offer advice to parents and students about mobile phones and social media via the website, InTouch, information evenings and through discussion with Student Services, Pastoral and Senior Staff. Where incidents of cyber-bullying or 'sexting' are reported, the school will investigate.

Scope

- Children's safety when using mobile phones and other internet enabled devices is the responsibility of parents, students and staff. We will therefore work together according to commonly agreed principles.

- We have an obligation to investigate incidents of bullying, including cyber-bullying, occurring in and out of school. (Preventing and Tackling Bullying, DfE 2017). Incidents involving mobile phones or social networks that happen outside of school will be investigated following the processes below.
- We have the right to confiscate and search devices as well as deleting files or images. (Education Act 2011). There are different processes followed depending on whether the mobile phone incident is one of a) Child Protection or b) a Safeguarding or Bullying issue.

Expectations

1. Students are taught about conduct on mobile phones and social networks, via PD lessons, assemblies and the pastoral curriculum. There is also guidance in their planners (see Appendix 2), and on the school website.
2. Parents should be aware of how their children are using their phones and social networks. We advise frank, open discussion so that parents are informed about what risks their children may be exposing themselves to in the digital world. There is also a wealth of advice and guidance for parents on the website: http://www.billericay.essex.sch.uk/parents/using-the-internet-and-smartphones-safely We expect students and their parents to follow advice about age recommendations for different social network sites and apps: https://www.net-aware.org.uk/
3. We expect parents to have talked to their children about privacy settings and advise that students in KS3 or 4 have private accounts to which only close friends and family are allowed access.
4. We will offer advice to parents and students about mobile phones and social media via the website, InTouch, information evenings and through discussion with Student Services, Pastoral and Senior staff.
5. We will investigate instances of child protection, safeguarding and bullying following the processes and protocols below. We can only investigate incidents effectively if parents have followed our advice about age restrictions, privacy settings and monitoring their child's phone use. The phone contract is usually in the parent's name and is, therefore, ultimately their responsibility.

Processes and Protocols

Student Services and Pastoral staff will only look at children's phones if directed to do so by a member of SLT. Students should not have phones in school and if they are seen or heard they will be confiscated. Phones may be searched if there is a disclosure that there are images, videos or text which are: a) potentially illegal and/or a child protection issue (e.g. an explicit image) or b) a safeguarding or cyber-bullying incident relating to an infringement of school rules (e.g. a fight in or out of school).

a) Child Protection Issues

- If a child discloses that an explicit image has been sent, received or shared (sometimes referred to as 'sexting'), normal safeguarding practices relating to disclosures will be followed. The UK Council for Child Internet Safety (UKCCIS) and CEOPS guidance documents will be consulted and adhered to. **The matter should be reported to Safeguarding, who will decide whether it is a police matter, according to the guidance (see Response Process Sheet).**

- If it is not a police matter, and the image is on the device the student will be asked to delete it. The phone will be confiscated and returned to the parent. Parents will be informed and advised. If the image has been shared on a social network site parents will be advised to report it to the site so it can be taken down. If the child is deemed to be at risk, it will be reported to CEOPs by the designated member of staff.

b) Safeguarding or Cyber-Bullying Incidents

- If a student or their parent reports bullying on social media, they will be advised to block the offending person and ensure they are following our guidance re privacy settings and age limits. If the incidents continue, or are being brought into school, parents may be asked to send in screenshots with information on usernames of all involved. Student Services will speak to students involved, remind them of our policy and expectations around bullying, mobiles and social networks and inform parents, if necessary, so sanctions can also be applied at home. If the incidents happened in school or are continuing offline as well as on, sanctions will be applied in school according to our Behaviour and Anti-Bullying Policies.
- If the cyber-bullying continues outside of school despite privacy settings and blocking measures put in place, and is deemed to be harassment, parents may be advised to report incidents to the police for them to determine whether there is a crime committed in terms of The Malicious Communications Act (1988).
- If an incident happened in or out of school and there is evidence on mobile phones, staff may confiscate and search devices with or without permission according to The Education Act (2011).
- Staff may use the school computers or a designated mobile device to investigate incidents where images, text or videos are placed online in the public domain, including those on students' public social media accounts.
- Student Services and pastoral Staff will not look through students' phones unless explicitly directed by a member of SLT.

SECTION 6

CYBER-BULLYING

WHAT IS CYBER-BULLYING?

The rapid development of, and widespread access to, technology has provided a new medium for 'virtual' bullying, which can occur in or outside school.

Cyber-bullying is a different form of bullying, but has a number of key differences, which can be summarised as follows:

- Bullying can happen 24/7 making it difficult to escape
- The audience for cyber-bullying is potentially much larger, increasing the impact
- Cyber-bullying incidents can quickly escalate making them difficult to contain
- Anonymity and being one step removed makes it easier for the bystander to join in
- Anonymity also increases the impact on those being bullied as they cannot be sure who is responsible
- There is a general lack of awareness that behaviour is cyber-bullying and young people tend to underestimate the impact of their behaviour
- Unlike traditional forms of bullying, evidence is readily available and should be preserved

THE LEGAL FRAMEWORK

As outlined in DfE guidance 'Preventing and Tackling Bullying'[1] (2014), teachers have the power to discipline pupils for misbehaving outside the school premises 'to such an extent as is reasonable'. DfE guidance 'Cyberbullying: Advice for Headteachers and School Staff'[2] (2014) outlines the importance of bullying (including cyber-bullying) being tackled as a 'community issue for the whole school', and goes on to state that, 'where bullying outside school is reported to school staff, it should be investigated and acted on'.

Section 89(5) of the Education and Inspections Act (2006) gives head teachers the power to regulate students' conduct when they are not on school premises and are not under the lawful control or charge of a member of school staff'.

In response to this advice and guidance, the school will investigate incidents of bullying (including cyber-bullying) when it is deemed appropriate.

[1] Preventing & Tackling Bullying: Advice for Headteachers, Staff & Governing Bodies (October 2014) https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/444862/Preventing_and_tackling_bullying_advice.pdf

[2] 'Cyberbullying: Advice for Headteachers and School Staff'[2] (November 2014) https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice_for_Headteachers_and_School_Staff_121114.pdf

INCIDENTS INVOLVING STUDENTS

The school’s response to cyber-bullying involving students is outlined in Section 5 above.

INCIDENTS INVOLVING STAFF

The schools response would be identify whether the matter is for further awareness of the effective use of modern technologies or action taken in relation to infringements of the staff AU policy.

SECTION 7

MISUSE OF NETWORK OR INTERNET

Sanctions for Misuse of Network or Internet

1. Abuse of the Internet (Playing arcade type games; downloading music files for personal use; using streaming video for personal use). An automatic 4-week Internet ban.
2. Allowing someone else to use your Internet access because they have been banned.

   An automatic 4-week Internet ban for the student allowing another student to use their Internet access

   A further-week Internet ban for the student accessing the Internet when banned. A letter will be sent home to the parents at this point.
3. A student who has been banned on three separate occasions will receive a 2-week network ban, a 1-term Internet ban and a letter home saying that a further breach would lead to a permanent ban from the Internet.
4. A student found abusing the network in any physical way such as damaging the keyboards, mice etc. will receive an automatic 2-week network ban, and an invoice to cover the cost of the item or items. There should also be a letter home outlining the circumstances, and the reasons for the ban.
5. A student found abusing the network in a physical way for a second occasion will receive a 6-week network ban, and an invoice to cover the cost of the item or items. There will also be a letter home outlining the circumstances, and the reasons for the ban.
6. Any further abuses would lead to further half-termly bans with the other conditions.

Sanctions for Accessing Pornography or Similar Serious Abuses

1. A student found to be searching for pornography, and /or printing the pictures will have an automatic 6-week Internet ban, a 2-week network ban, and a letter home to the parents explaining that the evidence is available if required.
2. A student found trying to access the school system by running executables will have a fixed term exclusion, and a 2-week network ban.
3. Any further abuse of this nature could lead to further exclusion, a permanent Internet ban, a 1-term network ban, and a letter home to the parents explaining that the evidence is available if required.

4. More serious breaches will be decided on individually by SLT and then fed back to the ICT department so that the punishment can be enforced.

SECTION 8

APPENDICES

APPENDIX 1a

ACCEPTABLE COMPUTER & INTERNET USE POLICY – STAFF

The computer system is provided by the school and is made available to students and staff to support and enhance their education, research and work at school. This Computer, Internet and ePortal Policy has been drawn up to protect all parties - the students, the staff and the school. Remember that access to the network resources and Internet is a privilege, not a right, and that access requires responsibility.

This policy also applies whenever information is accessed through the Billericay ePortal, whether the computer equipment used is owned by The Billericay School or not. The policy applies to all those who make use of The Billericay's ePortal Service.

- Staff will only use the school's email, internet, intranet and any related technologies for professional purposes;
- All Computer or Internet use should be for study purposes, and enhance your work done in the classroom. This means that games and radio / mp3 download sites are forbidden.
- Access should only be made via your authorised username and password which should not be shared; you alone are responsible for your user area. These usernames and passwords should ***never*** be disclosed to anyone.
- The disclosure of private, sensitive, and confidential information should not be allowed through the ePortal. Users should not attempt to access the ePortal system in any environment where the security of the information contained in the ePortal system may be placed at risk e.g. a cybercafé
- Information made available through the ePortal system is confidential and protected by law under the Data Protection Act 2018. To that aim: Users must not distribute or disclose any information obtained from the ePortal system to any person(s) with the exception of the pupil to which the information relates or to other adults with parental responsibility
- Activity that damages or changes the school computer systems, or activity that attacks or corrupts other systems, is forbidden and may be an offence under the Computer Misuse Act 1990;
- No programs may be brought in on disk or downloaded onto any machine; staff will not install any hardware or software without permission of the Network manager
- Copyright of materials must be respected; copying of software is not permitted;

- Users are responsible for all e-mail sent and for contacts made that may result in e-mail being received; messages should be polite and responsible; only school e-mail will be used;
- Do not reveal personal information, the home address or phone numbers of yourself or other people;
- The use of the computer network for personal financial gain, gambling, political purposes or advertising is forbidden;
- Posting anonymous messages and forwarding chain letters is forbidden;
- Use of the network to access inappropriate materials such as pornographic, racist or offensive material is forbidden.
- Electronic communications with pupils and staff are compatible with the professional role;
- Staff should not give out their own personal details such as mobile phone number, personal email address or social network identity to pupils;
- All school ICT equipment should be kept secure, whether in school or off site including travelling from and to work.
- Staff will only take/store or use pictures of pupils and/or staff only for professional purposes;
- Data Protection regulations should always be followed;
- The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet sites visited.

Yours sincerely,

A Mohammed Headteacher

✂……………………………………………………………………………………………

Please print
Staff Name: _________________________(Please Print)

Network Username: _______________________

As a school user of the Internet, I agree to comply with the school rules on its use. I will use the network in a responsible way and observe all the restrictions explained to me by the school.

Staff Signature: _____________________________

APPENDIX 2a

ACCEPTABLE COMPUTER & INTERNET USE POLICY – PARENTS & CARERS

This policy also applies whenever information is accessed through the Billericay e-Portal, whether the computer equipment used is owned by The Billericay School or not. The policy applies to all those who make use of The Billericay's e-Portal Service known nationally as the **Learning Gateway.**

E-Portal Usage Policy Rules

Authorised e-Portal Users

The Billericay School's e-Portal system is provided for use by persons who are legally responsible for pupil(s) currently attending the school.
Access is granted only on condition that the individual formally agrees to the terms of this Policy. The authorising member of school staff **must** confirm that there is a legitimate entitlement to access information for pupils the names of whom must be stated on the e-Portal Parental Access Request Form. A copy of the form will be held by the school for audit purposes. Requests for Access to the e-Portal system must be made to The Billericay School using the ePortal Parental Access Request Form.

Personal Use

Information made available through the e-Portal system is confidential and protected by law under the Data Protection Act 1998. To that aim:

- Users must not distribute or disclose any information obtained from the e-Portal system to any person(s) with the exception of the pupil to which the information relates or to other adults with parental responsibility
- Users should not attempt to access the e-Portal system in any environment where the security of the information contained in the e-Portal system may be placed at risk e.g. a cybercafé

Password Policy

You must assume personal responsibility for your username and password. Never use anyone else's username or password.
You must always keep your individual user name and password confidential. These usernames and passwords should ***never*** be disclosed to anyone. Passwords and user names should never be shared. In some instances users may be given the right to change the ePortal password from the one originally issued by the school. If this is the case the following rules must be followed:

- Passwords must be at least 6 characters (a-z, 0-9) in length

- Passwords must contain at least 1 number (0-9)
- Passwords must not be similar to your own name or username for example: cutler1

Questions, Complaints and Appeals

e-Portal users should address any complaints and enquiries about the e-Portal system to The Billericay School by email: parentportal@billericay.essex.sch.uk or telephone: 01277 655191

The Billericay School reserves the right to revoke or deny access to the e-Portal system of any individual under the following circumstances:

- The validity of parental responsibility is questioned
- Court ruling preventing access to child or family members is issued
- Users found to be in breach of the e-Portal usage policy

If any child protection concerns are raised or disputes occur the school will revoke access for all parties concerned pending investigation.

Please note: Where e-Portal access is not available The Billericay School will still make information available according to Data Protection Act (2018) law.
Users are liable for any potential misuse of the system and/or breach of the data protection act that may occur as a result of failing to adhere to any of the rules/guidelines listed in this document.

It would be much appreciated if you would give us an email address so that we can contact you regarding important information such as newsletters, parents evenings etc.

Yours sincerely,

Ahson Mohammed Headteacher

✂…………………………………………………………………………………………

Please print
Parent/ Guardian Name: __________________________(Please Print)

Childs Name: ________________________Tutor Group: ______________

Parental Signature: ______________________________

Email Address: _______________________________
Any problems relating to your use of the site should be emailed to **info@billericay.essex.sch.uk**

APPENDIX 3a

The Billericay School
Acceptable Computer and Internet Use Policy

The computer system is provided by the school and is made available to students and staff to support and enhance their education, research and work at school. This Computer and Internet Use Policy has been drawn up to protect all parties - the students, the staff and the school.

Remember that access to the network resources and Internet is a privilege, not a right, and that access requires responsibility.

Internet access is automatically given to the students when they arrive in school, unless the parents / guardians specifically ask otherwise. This should be in writing.

- All Computer or Internet use should be responsible, sensible and for study purposes, and enhance your work done in the classroom. This means that games and radio / mp3 download sites are forbidden.
- Access should only be made via your authorised username and password which should not be made available to any other person; you alone are responsible for your user area.
- Activity that damages or changes the school computer systems, or activity that attacks or corrupts other systems, is forbidden and may be an offence under the Computer Misuse Act 1990;
- No programs may be brought in on disk or downloaded onto any machine;
- Copyright of materials must be respected; copying of software is not permitted;
- Users are responsible for all e-mail sent and for contacts made that may result in e-mail being received; messages should be polite and responsible;
- Do not reveal personal information, the home address or phone numbers of yourself or other people;
- The use of the computer network for personal financial gain, gambling, political purposes or advertising is forbidden;
- Posting anonymous messages and forwarding chain letters is forbidden;
- Use of the network to access inappropriate materials such as pornographic, racist or offensive material is forbidden.
- The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet sites visited.
- Students will only take/store or use pictures of students and/or staff only for professional purposes.

Sanctions

1. Violation of the above rules will result in a temporary or permanent disabling of Internet and Computer network access.

2. Additional disciplinary action may be added in line with existing school expectations of behaviour.

3. When applicable, outside authorities may be involved.