PLASHET SCHOOL

Working together to promote & celebrate achievement

Online Safety Policy

Revised and applicable from 31st March 2022

Signed: Irene Papad

Chair of Governors

Introduction

Online safety is defined as:

- Promoting practices that allow safe use of the Internet
- Giving both students and staff agreed parameters for their use of ICT
- Online safety applies to all ICT use, including the fixed and mobile technologies and to both on-line and off-line ICT usage.
- Safeguarding information held using ICT systems.

Plashet School is committed to providing ICT access safely and responsibly. We believe that:

- All students have the right to use ICT equipment in a safe and controlled environment.
- All students should be taught to manage and minimise risks of being on-line.
- Staff have a key role in educating students to be responsible digital citizens.
- Staff in their own use of ICT should practice safe and responsible working practices.

New technologies have become integral to the lives of young people in today's society, both within educational establishments and in their lives outside school. The Internet and other digital/information technologies are powerful tools which open up new opportunities for everyone. Electronic communication helps teachers and students learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Young people should have an entitlement to safe Internet access at all times. The requirement to ensure that young people are able to use the Internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. This online safety policy will help to ensure safe and appropriate use. The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote student achievement. However, the misuse of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content.
- Unauthorised access to, loss of or sharing of personal information.
- The risk of being subject to grooming by those with whom they make contact on the Internet.
- The sharing/distribution of personal images without an individual's consent or knowledge.
- Inappropriate communication/contact with others, including strangers.
- Cyber-bullying.
- Access to unsuitable video/Internet games.
- An inability to evaluate the quality, accuracy and relevance of information on the Internet.
- Plagiarism and copyright infringement.
- Illegal downloading of music or video files.
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this online safety policy is read and used in conjunction with other school policies; specifically: Student Code of Conduct, Home-School Agreement, Staff Code of Conduct, Staff Guidance on Safer Working Practices, Anti-Bullying, Behaviour, Community Resilience and Safeguarding.

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision, to build students' resilience to the risks to which they may be exposed so that they have the confidence and skills to face and deal with these risks.

The school provides the necessary safeguards to help ensure that we have done everything that could reasonably be expected to manage and reduce these risks. The online safety policy explains how the school intends to do this, whilst also addressing wider educational issues in order to help young people (and their parents/carers/staff) to be responsible users and stay safe while using the Internet and other communications technologies for educational, personal and recreational use.

Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of students, staff, volunteers and governors.
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology.
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scam.

Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

Scope

This policy applies to all members of the school community (including staff, students, governors, volunteers, parents/carers and visitors) who have access to and are users of school ICT systems, both in and out of school. The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other online safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school. The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school. However, it should be reiterated that the primary responsibility for the welfare of students outside school is with parents and carers.

Roles & Responsibilities

This section outlines the roles and responsibilities for online safety of individuals and groups within the school.

The school has an Online Safety Coordinator. This person liaises with the Designated Safeguarding Lead, Safeguarding Officers and the Community Resilience single point of contact (SPOC) as and when the roles overlap.

Governors

Plashet School's Online Safety Policy has been written by the school, building on government guidance. It has been agreed by the Leadership Team and approved by governors. The Online Safety Policy and its implementation will be reviewed annually. A member of the Governing Body should take on the role of Online Safety Governor. The role of the online safety Governor will include:

- Meetings with the Online Safety Coordinator.
- Regular monitoring of online safety serious incident logs.
- Monitoring of effectiveness of Securus and Securly software.
- Reporting to the relevant Governing Board and/or committee at meetings.

Head Teacher & Leadership Team (LT)

The Head Teacher is responsible for ensuring:

- The safety (including online safety) of all members of the school community, although the day-to-day responsibility for online safety may be delegated to the Online Safety Coordinator who is a member of the LT.
- Adequate training is provided.
- Effective monitoring systems are set-up.
- That relevant procedure in the event of an online safety allegation is known and understood.
- Establishing and reviewing the school online safety policies and documents (in conjunction with Online Safety Coordinator).
- The school's Designated Safeguarding Lead and Safeguarding Officers should be trained in online safety issues and be aware of the potential for serious child protection issues that could arise through the use of ICT.

Online Safety Coordinator

The Online Safety Coordinator takes day-to-day responsibility for online safety issues and has a leading role in:

- Liaising with staff, IT managed service staff, Police, LBN, administrative staff, pastoral staff, Online Safety Governor and LT on all issues related to online safety;
- Ensuring that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place;
- Providing training and advice for staff;
- Receiving reports of serious online safety incidents and creating a log of incidents to inform future online safety developments;
- Co-ordinating and reviewing online safety education programmes in school
- Promoting online safety with parents and the local community.

The Designated Safeguarding Lead

Details of the school's DSL and deputy are set out in our child protection and safeguarding policy.

The DSL takes lead responsibility with the Online Safety Coordinator for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school.
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents.
- Managing all online safety issues and incidents in line with the school child protection policy.
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyberbullying are logged and dealt with appropriately in line with the school behaviour policy.
- Updating and delivering staff training on online safety.
- Liaising with other agencies and/or external services if necessary.
- Providing regular reports on online safety in school to the headteacher and/or governing board.

This list is not intended to be exhaustive.

ICT Managed Service

Plashet School currently has an IT managed service to manage the ICT infrastructure in school.

The IT managed service staff are responsible for ensuring that:

- The school's ICT infrastructure is secure and meets online safety technical requirements.
- The school's password policy is adhered to.
- The school's filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.
- They keep up to date with online safety technical information.
- The use of the school's ICT infrastructure (network, remote access, e-mail etc.) is regularly monitored in order that any misuse or attempted misuse can be reported to the Online Safety Coordinator and/or LT for investigation/action/sanction.
- Monitoring software is kept up to date.
- School chromebooks are made available for distribution to staff and students and Acceptable User Agreements (AUA) are signed and filed.

Teaching & Support Staff
In addition to elements covered in the Staff ICT Accessible Use Guidelines and the Chromebook Acceptable Use Agreement, all teaching and support staff are responsible for ensuring that:

- They have an up to date awareness of online safety matters and of the current school online safety policy and practices.
- They have read, understood and signed the school Staff ICT Accessible Use Guidelines.
- They have read, understood and signed the school Chromebook Acceptable Use Agreement.
- Online safety issues are embedded in all aspects of the curriculum and other school activities.
- Students understand and follow the school's online safety and acceptable usage policies.
- Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- They monitor ICT activity in lessons and extended school activities.
- In lessons where Internet use is pre-planned, students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in Internet searches.

Students

- Are responsible for using the school ICT systems in accordance with the Student Acceptable Usage Policy, which they will be required to sign before being given access to school systems. Parents/carers will be required to read through and sign alongside their child's signature.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's online safety policy also covers their actions out of school, if related to their membership of the school.

Parents/Carers
Parents/Carers play a crucial role in ensuring that their children understand the need to use the Internet /mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take opportunities to help parents understand these issues. Parents and carers will be responsible for:

- Endorsing (by signature) the Student Acceptable Usage Policy.
- Accessing the school website in accordance with the relevant school Acceptable Usage Policy.

Parents and carers need to be proactive in discussing the opportunities and risks associated with online activity. Some of the key discussion points that parents may want to discuss with their children are:

- What is the appropriate age for children to have a smartphone?
- Are there minimum age limits for certain apps, social networking sites and video games?
- What monitoring software is being used at home to monitor online activity through the home IP address?
- Are there certain sites that should be blocked from your home Wi-Fi? (Contact your Internet Service Provider for further details).
- If children are playing games online with an online gaming community element, who is part of that community?

- Are you familiar with all the apps on your child's smartphone or desktop/laptop and what their main purpose is? (Some apps have been specifically designed to post anonymous comments about individuals which lends itself to cyber bullying).

Parents can seek further guidance on keeping children safe online from the following organisations and websites:
What are the issues? – UK Safer Internet Centre
Hot topics – Childnet International
Parent resource sheet – Childnet International
Healthy relationships – Disrespect Nobody

Additional Users
Community Users who access school ICT systems/website/Learning Platform as part of the curricular or extracurricular provision will be expected to sign the Staff & Visitor Acceptable User Agreement (see Appendix 6) before being provided with access to school systems.

Education and Training

Students will be taught about online safety as part of the curriculum:
In Key Stage 3, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

Pupils in Key Stage 4 will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

By the end of secondary school, pupils will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including prison
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

Learning and development will be provided in the following ways:

- A planned online safety programme is provided as part of the form tutor and assembly programme and is regularly revisited in Information Technology and other lessons across the curriculum – this programme covers both the use of ICT and new technologies in and outside of school.
- Digital Resilience is taught through the Citizenship, Learning for Life and Computing Curriculums. (See Appendix 8 Promoting Digital Resilience)
- Students are taught in lessons to be critically aware of the materials/content they access online and are guided to validate the accuracy of the information.
- Students are helped to understand the need for the Student Acceptable Use Policy (AUP) and encouraged to adopt safe and responsible use of ICT, the Internet and mobile devices both within and outside of school.
- Students are taught to acknowledge the source of information used and to respect copyright when using material accessed on the Internet.
- Rules for the use of ICT systems and the Internet are posted in school.
- Staff act as good role models in their use of ICT, the Internet and mobile devices.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some students with SEND.

Cyber-bullying

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that students understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with students, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Form teachers will discuss cyber-bullying with their tutor groups as will Learning for Life teachers.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support students, as part of safeguarding training (see section 11 for more detail).

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in Appendix 1 and in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The Online Safety Coordinator and DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on students' electronic devices, including mobile phones where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the Online Safety Coordinator or DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police*

* Staff may also confiscate devices for evidence to hand to the police, if a student discloses that they are being abused and that this abuse includes an online element.

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on screening, searching and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- The school's COVID-19 risk assessment

Any complaints about searching for or deleting inappropriate images or files on students' electronic devices will be dealt with through the school complaints procedure.

Students using mobile devices in school

Students may bring mobile devices into school, but the device must remain switched off as they are not permitted to use them on the school premises.

Acceptable Use Agreement

- **Parents/carers** will be required to read through and sign alongside their child's signature, helping to ensure their children understand the rules
- **Staff** have an AUP that they must read through and sign to indicate understanding of the rules.

Copyright

- Students to be taught an appropriate understanding of research skills and the need to avoid plagiarism and uphold copyright regulations - staff to monitor this.
- Students are taught, appropriate to their age, to acknowledge the source of information used and to respect copyright when using material accessed on the Internet.

- If using a search engine for images – staff/students should open the selected image and go to its website to check for copyright.

Staff

- Online safety coordinator ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- All staff undertake annual training via the school's EduCare online programme.
- The Online Safety Coordinator will receive regular updates through Local Authority and/or other information/training sessions and by reviewing guidance documents released.
- Governors are invited to take part in online safety training and awareness sessions, with particular importance for those who are members of any committee or working group involved in ICT, online safety, health and safety or child protection.

Communication

Email

- Digital communications with students should be on a professional level only and only carried out using official school systems, namely via G Suite.
- Under no circumstances should staff contact students, parents/carers or conduct any school business using personal email addresses.
- School email is not to be used for personal use. Staff can use their own email in school (before, after school and during lunchtimes when not working with children) but not for contact with parents/students.

Mobile Telephones

- School mobile telephones only should be used to contact parents/carers/students when on school business with students off site. Staff should not use personal mobile devices.
- Staff should not use personal mobile telephones in school during working hours when in contact with children.
- Students should adhere to the rules and guidelines set out in the Behaviour Policy regarding no mobile telephone use being allowed in school.

Social Networking Sites

Young people will not be allowed on social networking sites at school; at home it is a parental responsibility and parents need to be proactive in ensuring the content their children are accessing or posting online is suitable. Parents should be aware that it is illegal for children under the age of 13 to be on certain social networking sites.

- Staff should not access social networking sites on school equipment in school.
- Staff users should not reveal the name of the school or names of staff, students, parents/carers or any other member of the school community on any social networking site or blog**.**
- Students/Parents/Carers should be aware that the school will investigate misuse of social networking if it impacts on the well-being of other students or stakeholders in school. It is, however, the responsibility of parents to monitor the usage of their children's digital communication outside school.
- If inappropriate comments are placed on social networking sites about the school or school staff, advice would be sought from the relevant agencies, including the police if necessary.

Digital Images

- The school's records of parental permissions granted/not granted must be adhered to when taking images of our students. This information can be obtained from the school's management SIMS system.
- Under no circumstances should images be taken using privately owned equipment without the express permission of the Head Teacher or the Online Safety Coordinator.
- Where permission is granted, the images must be uploaded to the relevant place on Google Drive and deleted from mobile equipment at the earliest opportunity.

Removable Data Storage Devices

- Staff should be using G Suite for Education to manage workflows. USBs and portable storage devices are not encouraged as they can increase the risk of transferring viruses or GDPR breaches. If a portable storage device really needs to be used, staff must ensure it is a 'clean' device which is not used with other high risk devices like public computers.
- All files downloaded from the Internet, received via e-mail or provided on removable media (e.g. CD, DVD, USB flash drive, memory cards etc.) must be checked for viruses using school provided anti-virus software before run, opened or copied/moved on to local/network hard disks.

Websites

- In lessons where Internet use is pre-planned, students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in Internet searches.
- Staff should check the results of "Open" searches in advance (e.g. "find images/ information on...") to ensure inappropriate images or information does not come up on the computer screen. In such cases, staff should advise students to modify their searches to ensure appropriate images or information come up on their computer screens.
- All staff have a responsibility that if they pass students working on the Internet that they have a role in checking what is being viewed. Students are also aware that all Internet use at school is tracked and logged.

Passwords

Staff

- Passwords or encryption keys should not be recorded on paper or in an unprotected file
- Users should not use the same password on multiple systems or attempt to "synchronise" passwords across systems

Students

Should protect their password at all times and never share it. Students are responsible for keeping their passwords secure and will be held responsible for any online activity which occurs under their account. They inform staff immediately if passwords are traced or forgotten and it will be reset using the IT managed service.

Use of Equipment

Use of Own Equipment

- Privately owned ICT equipment should never be connected to the school's network without the specific permission of the Head Teacher or Online Safety Coordinator.
- Students should not bring in their own equipment unless authorised to do so by a senior member of staff.

Use of School Equipment

- No personally owned applications or software packages should be installed on to school ICT equipment;
- Personal or sensitive data (belonging to staff) should not be stored on the local drives of desktop or laptop PCs.
- All should ensure any screens are locked (by pressing Ctrl, Alt, Del simultaneously) before moving away from a computer during the normal working day to protect any personal, sensitive, confidential or classified data and to prevent unauthorised access.

Monitoring

All use of the school's Internet access and keyboard activity is monitored using the Securus software. Whenever any inappropriate use is detected, office staff alert the relevant staff member of the classroom where the breach took place and it is dealt with using the behaviour policy. Where the breach is considered especially serious, it will be followed up by the Online Safety Coordinator. Staff and student activity on the chromebook devices is monitored by the Securly software. Whenever any inappropriate use is detected, the administrator with oversight will alert the relevant staff member depending on the nature of the inappropriate content.

Incident Reporting

Serious student online safety incidents must be reported to the Online Safety Coordinator who will investigate further following online safety and safeguarding policies and guidance. If the concern relates to a member of staff it should be reported to the Head Teacher.

Responding to incidents of misuse

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place through careless or irresponsible, or very rarely, through deliberate misuse. If any apparent or actual misuse appears to involve illegal activity, e.g. child sexual abuse images, sharing of nudes or semi-nudes, adult material which potentially breaches the Obscene Publications Act, criminally discriminatory material or other criminal conduct, activity or materials, Appendix 1 should be consulted. Actions will be followed in accordance with policy, in particular the sections on reporting the incident to the police and the preservation of evidence. If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above), it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. It is recommended that more than one member of staff is involved in the investigation, which should be carried out on a "clean" designated computer. It is important that any incidents are dealt with as soon as possible, in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures.

Appendix 1

Online Safety Incident Procedure

An online incident is where our school monitoring systems have filtered web-activity leading to a well-being or safeguarding concern for a student or where there has been some misuse of social media or digital technology. This policy must be read in conjunction with the school safeguarding policy and the school behaviour policy.

Online Incidents can occur in the following contexts:

1) Outside of school hours using school chromebook devices (monitored by Securly)
2) Inside school hours using school IT infrastructure (monitored by Securus)
3) Outside of school hours using student personal devices (identified through investigations into behavioural incidents or disclosures relating to the well-being or safeguarding of a student).
4) Inside school hours using student personal devices.

Outside of school hours using school chromebook devices (monitored by Securly) and Inside school hours using school IT infrastructure (monitored by Securus)

Securly and Securus alerts are automatically generated based on the school filtering system and monitored by a member of the admin team in school. The School's Data Lead will complete an initial assessment. If the alert requires no further investigation the alert is closed.

If the alert has a well-being or safeguarding implication the member of the admin team completes the following and forwards to the YC, AYC/ LT Line Manager and safeguarding lead for the year group:

a. Full name of student
b. Form
c. Brief description of incident

The pastoral team will then make a secondary assessment in consultation with the well-being mentors if the alert requires further investigation. If further investigation is required the student will be spoken to and a safeguarding referral will be made.

Outside of school hours using student devices (identified through investigations into behavioural incidents)

Where a behaviour incident has occurred and there has been some misuse of social media or digital technology, the pastoral team will complete an alert for the incident including:

a. Full name of student
b. Form
c. Brief description of incident

The pastoral team will then implement school based sanctions and the parents/guardians will be contacted and advised to take the following steps based on the seriousness of the incident. Incidents can be categorised into 3 levels:

Level 1 (low level violation): A student has been accessing inappropriate social media platforms commonly used for cyber bullying or accessing social media platforms which are not age appropriate. Students may also be using inappropriate language online.

Action: Student given a warning by the pastoral team and parents/carers contacted and asked to speak to their daughter.

Level 2 (medium level violation): A student has been involved in inappropriate use of social media which has led to a behavioural incident in school. A student may also be accessing inappropriate websites eg gaming.

Action: Student given a school based sanction by the pastoral team and parents/guardians contacted and asked to implement corrective measures with their daughter at home which include the following:

- Installing monitoring software on home Wi-Fi
- Implementing a digital sunset time where device use is out of bounds
- Checking through all the apps on their daughter's device and deleting inappropriate apps commonly used for cyber bullying
- Checking that their daughter is not communicating online with any contacts who she does not know in person
- Removing apps from their device that are being used as a platform for cyber bullying or any other form of misuse.

Level 3 (high level violation): Student has been involved in inappropriate use of social media which has led to a serious behavioural incident in school. Students may also be using social media to mock or ridicule students or staff or be expressing hate speech.

Action: Student given a serious school based sanction (internal isolation or exclusion) and the device involved in the misuse is confiscated by parents/guardians:

- If the device is a school chromebook the password is temporarily blocked by the school.
- If the device is a personal device parents/guardians confiscate the relevant device at home. The school can support this and the school safe can be used for safe storage.

Parents/Guardians are then advised to implement the medium term corrective measures once the device is returned.

Inside school hours using student personal devices.

If a student personal device is seen or heard on school grounds it is automatically confiscated for 3 school days and kept for safe storage in the school safe in South reception. A letter will be sent to parents/guardians informing them of the device use. There is no requirement to discuss whether the phone was being used or not. Any instance of the device being seen or heard will lead to confiscation. A student who refuses to hand their device to school staff will be in defiance of school rules and the behaviour policy will apply.

Appendix 2

Plashet School Frequently Asked Questions for Parents

Why is Internet use important?

- Internet use is part of the statutory curriculum and a necessary tool for learning.
- The Internet is a part of everyday life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.
- Students use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.
- The purpose of Internet use in school is to raise educational standards, to promote student achievement, to support the professional work of staff and to enhance the school's management functions.
- Internet access is an entitlement for students who show a responsible and mature approach to its use.

How does Internet use benefit education?

Benefits of using the Internet in education include:

- access to worldwide educational resources including museums and art galleries;
- educational and cultural exchanges between students worldwide;
- vocational, social and leisure use in libraries, clubs and at home;
- access to experts in many fields for students and staff;
- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- collaboration across networks of schools, support services and professional associations;
- improved access to technical support including remote management of networks and automatic system updates;
- exchange of curriculum and administration data with London Borough of Newham (LBN) and Department for Education (DfE);
- Access to learning wherever and whenever convenient.

How can Internet use enhance learning?

- The school's Internet access will be designed to enhance and extend education.
- Students will be taught what is and isn't acceptable in terms of Internet use and given clear objectives for Internet use.
- The schools will ensure that the copying and subsequent use of Internet derived materials by staff and students complies with copyright law.
- Access levels will be reviewed to reflect the curriculum requirements and age of students.
- Staff should guide students to online activities that will support the learning outcomes planned for the students' age and maturity.
- Students will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Students will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

How will information systems security be maintained?

- The security of the school information systems and users will be reviewed regularly.
- Virus protection will be updated regularly.
- Personal data sent over the Internet or taken off site will be encrypted.
- Portable media may not be used without specific permission followed by a virus check. No unapproved software may be executed from portable media.
- Unapproved software will not be allowed in students' work areas or attached to email.
- Files held on the school's network will be regularly checked; media files that contravene copyright will be removed.
- The IT Support team will review system capacity regularly.
- Student user areas are provided by the school for students to save files relating to their studies. These are not private storage areas in the same way a student exercise book is not private. The

school reserves the right to review the files stored in student user areas as required.***Please refer to the school's data security policy for further information***

How will email be managed?

- Students may only use approved email accounts.
- Students must immediately tell a teacher if they receive an offensive email.
- Students must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an appropriate adult.
- Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain messages is not permitted.
- When communicating with students' staff should only use the systems provided and managed by the school via G Suite for Education.

How will published content be managed?

- The contact details on the website are the school address, email and telephone number. Staff or students' personal information must not be published.

- The Head Teacher will take overall editorial responsibility and ensure that content is accurate and appropriate. This task will be delegated to the Assistant Head Teacher with oversight for the school website and Twitter account.

Can student's images or work be published?

- Images that include students will be selected carefully and will not provide material that could be reused.
- Students' full names will not be used anywhere on the website, particularly in association with photographs.
- Written permission from parents or carers will be obtained before images of students are electronically published.
- Students' work can only be published with their permission or the parents.
- Students' images may be used within the school as part of a learning activity without parental permission (e.g. a video assessment of a drama piece, photos of an experiment taking place), but images will only be stored on school systems for the period of time that the learning activity requires them and deleted afterwards. Images will not be made available to students outside the group specifically engaged in the planned learning activity.

How will social networking, social media and personal publishing be managed?

- The school will control access to social media and social networking sites from all networked technologies.
- Students will be encouraged to consider the range of risks that are known to be associated with social networking systems. Students will be advised to always limit and carefully manage their privacy settings.
- Students will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs etc.
- Students should be advised to understand the dangers inherent with placing personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should include an understanding of how the background details in a photograph could identify the student or his/her location.
- Staff official blogs or wikis should be password protected and linked to, or hosted within, the school website with approval from the Leadership Group. Staff should be advised not to run social network spaces for student use on a personal basis.
- Staff should be advised that personal social networking and media systems should not be publicly associated with the school and should understand that bringing their profession and/or their employer into disrepute will result in disciplinary proceedings.
- If personal publishing is to be used with students, then it must use age appropriate sites suitable for educational purposes. Personal information must not be published and the site should enable moderation by school staff.

- Students should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Students should be encouraged to invite known friends only and deny access to others by making profiles private.
- Students are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.

How will filtering be managed?

- The school will work with LBN and our managed service provider to ensure that systems to protect students are reviewed and improved.
- If staff or students discover unsuitable sites, the URL must be reported to the Online Safety Coordinator.
- If inappropriate sites have been deliberately accessed the school will initiate disciplinary proceedings and/or sanctions as required. If the sites are potentially illegal or a part of a pattern of behaviour the school will involve appropriate safeguarding, law enforcement and local authority professionals. The school's broadband access includes filtering appropriate to the age and maturity of students.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- The school's access strategy will be designed by educators to suit the age and curriculum requirements of the students, with advice from network managers.
- The school monitors students' use of the internet through software that flags up keywords that are used in search engines, websites and browsers. A screenshot is captured and recorded as evidence.

How will emerging technologies be managed?

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones should be kept out of sight during the school day. Phones may be used to support learning in exceptional circumstances at the discretion of the Head Teacher. The sending of abusive or inappropriate text, picture or video messages is forbidden.
- Should a student or staff member report abusive or inappropriate messages on a personal mobile device the school should (with the owner's permission) photograph the message and follow the school's anti-bullying procedures. Should you suspect that the message is illegal (racist, threatening, etc.) you should isolate the device securely and take advice from local authority, law enforcement and safeguarding colleagues.

How should personal data be protected?

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018.

How will the school community be protected from extremism and radicalisation?

- Individuals, groups and organisations with extremist and radicalised views use the internet to exert influence on young people.
- Staff and students are prohibited from accessing any websites or social network pages that promote such views.
- The school has systems and filtering in place to block extremist material and monitor those who attempt to access it.
- Any persons deemed to be accessing extremist material will be reported to the relevant authorities.
- Refer to the school's Safeguarding Policy & Community Resilience Policy for more information.

How will Internet access be authorised?

- The school will maintain a current record of all staff and students who are granted access to the school's electronic communications.
- Parents will be informed that students will be provided with supervised internet access, together with guidance of what the school considers to be Acceptable Use.

How will risks be assessed?

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the

school nor LBN can accept liability for the material accessed, or any consequences resulting from internet use.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimise risks will be reviewed regularly.

How will Online/ESafety incidents be handled?

- Students are made aware of the various means to report an incident. These include: Informing a parent; informing a teacher (e.g. tutor/year coordinator); Asking a friend to tell an adult.
- Staff are made aware of the signs that might indicate abuse, bullying or harassment.
- If a child or teacher is in immediate danger the school's DSLS and police liaison officer will be contacted.
- If there is concern about the potential illegality of the issue, external advice from appropriate professionals will be sought.
- Involvement in online extremist activity or concerns about radicalisation of students will be discussed with the appropriate LBN team.
- Otherwise the school will manage incidents using the schools sanctions, disciplinary and/or anti-bullying policies as appropriate to the situation.
- All complaints related to online safety and incidents will be recorded by the school — including any actions taken.
- All incidents involving staff must be referred to the Head Teacher.
- Dialogue will be maintained with the school's Safer Schools Police Officer and/or LBN Safeguarding team to review procedures for handling potentially illegal issues.
- Complaints about the school's management of an online safety incident will be dealt with under the School's Complaints Procedure.

How will Cyber bullying be managed?

- Cyber bullying (along with all forms of bullying) will not be tolerated in school. Full details are set out in the school's anti-bullying policy.
- There are clear procedures in place to support anyone affected by cyberbullying.
- All incidents of cyber bullying reported to the school will be recorded.
- There are procedures in place to investigate incidents or allegations of cyber bullying.
- Students, staff and parents/carers will be advised to keep a record of the bullying as evidence.
- The school will take steps to identify the bully/bullies, where appropriate, such as examining system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Sanctions for those involved in Cyberbullying are set out in the school's behaviour policy.
- The Police will be contacted if a criminal offence is suspected.

How will the policy be introduced to students?

- All users will be informed that network and internet use will be monitored.
- Online is included within the assembly programme through which students will be made aware of current issues and will be reminded of the importance of safe and responsible internet use. This includes participating in Safer Internet Day.
- Student instruction in responsible and safe use shall precede internet access.
- An online module will be included in the ICT schemes of learning, covering both safe school and home use.
- Online training forms part of the Learning for Life programme across the Key Stages.
- Safe and responsible use of the internet and technology will be reinforced across the curriculum. Particular attention will be given where students are considered to be vulnerable.

How will the policy be discussed with staff?

- The Online Safety Policy will be formally provided to all members of staff.
- To protect all staff and students, the school will implement Acceptable Use Agreements.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user, Discretion and professional conduct is essential.
- Staff that manage filtering systems or monitor ICT use will be supervised by the Leadership Team and have clear procedures for reporting issues.
- Externally-verified, annual staff training covering all aspects of online safety will be provided.
- Staff updates are issued as and when appropriate.

How will parents' support be enlisted?

- Parents' attention will be drawn to the School Online Safety Policy in newsletters, via email and on the school website.

- A partnership approach with parents is encouraged. This includes: parent meetings with demonstrations and suggestions for safe home Internet use; regular updates and newsletters emailed home; Parent magazines set home with the students from telecommunication companies.

Appendix 3

Permissions to Use Communication Technologies

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks/disadvantages:

	Staff and other adults					**Students and young people**			
Communication Technologies	Permitted	Permitted at certain times	Permitted for named staff	Not Permitted		Permitted	Permitted at certain times	Allowed with staff permission	Not Permitted
Mobile telephones May be brought to school	✓								✓
Mobile telephones used in lessons				✓					✓
Use of mobile telephones in social time	✓								✓
Taking photographs on personal mobile devices				✓					✓
Use of school tablets & other educational mobile devices in lessons	✓					✓			
Use of school email for personal emails				✓					✓
Social use of chat rooms/facilities				✓					✓
Use of commercial social network sites			✓						✓
Use of educational blogs	✓					✓			

When using communication technologies, the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Staff and students should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users need to be aware that email communications may be monitored.
- Users must immediately report to the nominated person (in accordance with the school policy) the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and students or parents/carers (email, chat, Learning Platform etc.) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat/social networking programmes must not be used for these communications.
- Students should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Appendix 4

Inappropriate Activities

Some Internet activity, e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other ICT systems. Other activities, e.g. Cyber-bullying would be banned and could lead to criminal prosecution. There are, however, a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities. The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts certain Internet usage as follows. Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

User actions	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Child sexual abuse images					✓
Promotion or conduct of illegal acts, e.g. under the child protection, obscenity, computer misuse and fraud legislation					✓
Adult material that potentially breaches the Obscene Publications Act in the UK					✓
Criminally racist material in the UK					✓
Pornography					✓
Promotion of any kind of discrimination				✓	
Promotion of racial or religious hatred					✓
Threatening behaviour, including promotion of physical violence or mental harm					✓
Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				✓	
Using school systems to run a private business				✓	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by BMBC and/or the school				✓	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties without the necessary licensing permissions				✓	
Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords)				✓	
Creating or propagating computer viruses or other harmful files				✓	

Carrying out sustained or instantaneous high volume network traffic (downloading/uploading files) that causes network congestion and hinders others in their use of the Internet				✓	
On-line gaming (educational)		✓			
On-line gaming (non-educational)				✓	
On-line gambling				✓	
On-line shopping/commerce			✓		
File sharing			✓		
Use of social networking sites			✓		
Downloading video broadcasting e.g. YouTube	✓				
Uploading to video broadcast e.g. YouTube			✓		

Appendix 5

Online Safety Student Incident Guidance

The guidance in this policy should be implemented with cross reference to the School's Child Protection, Anti-Bullying and Behaviour Policies.

Incident involving students	**Teacher to use school behaviour policy to deal with**	**Refer to Online Safety Coord**	**Refer to police**	**Refer to IT managed service for technical support**
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/ inappropriate activities).		✓	✓	✓
Unauthorised use of non-educational sites during lessons	✓			✓
Unauthorised use of mobile telephone/digital camera/other handheld device.	✓			
Unauthorised use of social networking/instant messaging/personal email	✓	✓		✓
Unauthorised downloading or uploading of files		✓		✓
Allowing others to access school network by sharing username and passwords		✓		✓
Attempting to access or accessing the school network, using another student's account		✓		✓
Attempting to access or accessing the school network, using the account of a member of staff		✓		✓
Corrupting or destroying the data of other users		✓		✓
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		✓		✓
Continued infringements of the above, following previous warnings or sanctions		✓	Community Police Officer referral	✓
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		✓		✓
Using proxy sites or other means to subvert the school's filtering system		✓		✓
Accidentally accessing offensive or pornographic material and failing to report the incident		✓		✓

Appendix 6

Online Safety Staff/Visitor Incident Guidance

Incidents involving members of staff ***** In the event of breaches of policy by the Headteacher, refer to the Chair of Governors.	**Refer to the Head Teacher**	**Refer to technical support staff for action on filtering, security etc.**	**HT Referral to LBN LADO** **Potential Disciplinary Action**
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable /inappropriate activities).	✓	✓	✓
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	✓		✓
Excessive or inappropriate personal use of the Internet /social networking sites/ instant messaging/ personal email	✓	✓	✓
Unauthorised downloading or uploading of files	✓	✓	✓
Allowing others to access school networks by sharing username and passwords or attempting to access or accessing the school network, using another person's account.	✓	✓	✓
Careless use of personal data e.g. holding or transferring data in an insecure manner	✓		✓
Deliberate actions to breach data protection or network security rules	✓	✓	✓
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	✓	✓	✓
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	✓	✓	✓
Using personal email/ social networking/ instant messaging/ text messaging to carrying out digital communications with students/ students	✓	✓	✓
Actions which could compromise the staff member's professional standing	✓		✓
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	✓		✓
Using proxy sites or other means to subvert the school's filtering system	✓	✓	✓
Deliberately accessing or trying to access offensive or pornographic material	✓	✓	✓
Breaching copyright or licensing regulations	✓	✓	✓
Continued infringements of the above, following previous warnings or sanctions	✓		✓

Appendix 7

Student Acceptable Internet Use Agreement

This document is a guide to young people to be responsible and stay safe whilst using the Internet and other communication technologies. It clearly states what use of computer resources is acceptable and what is not. Irresponsible use may result in the loss of Internet or computer access, contact with parents or in the event of illegal activities, contact with the police.

- I will only access the school network through my authorised username and password. I will not use the passwords of others.
- I will not use the school IT systems for personal or recreational use, for on-line gaming, gambling, Internet shopping, and file sharing or video broadcasting.
- I will not try to upload, download or access any materials which are illegal, inappropriate or which may cause harm and distress to others.
- I will not try to use any programmes or software that might allow me to bypass the filtering and security systems in place.
- I will not try to install programmes on any school computer or try to alter computer settings.
- I will only use my personal hand held devices (e.g. mobile telephone) at times that are permitted, namely, for commuting to and from school or to contact parents after participation in an extracurricular activity or educational visit. When using my own devices I understand that I have to follow the rules set out in this document.
- I will carefully write email and other on-line messages making sure the language I use is not strong, aggressive or inappropriate and shows respect for others. I am responsible for the emails I send and the contacts I make.
- I will not open emails unless I know and trust the person/organisation that has sent them.
- For my own safety and that of others, I will not disclose personal information about myself or others when on-line. I will not arrange to meet 'on-line friends' unless I take an adult.
- I will not take or distribute images of anyone without their permission.
- I will only use chat and social networking sites with permission and at the times that are allowed.
- I will report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.
- Where the material I research on the Internet is protected by copyright, I will not try to download copies, including music and video. I will only use the work of others found on the Internet in my own work with their permission.
- I will take care to check that information I find on the Internet is accurate and understand that some work found on the Internet can be untruthful or misleading.
- I will immediately report any damage or faults involving IT equipment, however this may have happened.

Signed: ……………………………………………………………………………………………..

Date: ……………………………………

Appendix 8

Staff & Visitor Acceptable Internet Use Agreement

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 are powerful tools, which open up new opportunities for everyone. These technologies can inspire discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users have an entitlement to safe Internet access at all times.

This document 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.
- All Plashet ICT systems users are protected from accidental or deliberate misuse that could put the security of the systems or users at risk.
- 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 improve learning opportunities for all and will, in return, expect staff and volunteers to agree to be responsible users.

Responsible Use Agreement

I understand that I must use Plashet 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 learners 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 online safety in my work with students.

For my professional and personal safety:

- I understand that the school will monitor my use of school ICT systems, email and other digital communications.
- I understand the rules set out in this agreement also apply to the use of the school ICT systems (e.g. laptops, iPads, G Suite for Education) outside of the school.
- I understand that the school ICT systems are primarily intended for educational use and that I will only use systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username and 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/incident I become aware of to the appropriate person (see incident guidance grids in appendices 4 and 5).

I will be professional in my communications and actions when using school ICT systems:

- 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 equipment to record these images.
- I will not use chat and social networking sites in the school in accordance with the school's policies.
- I will only communicate with students and parents/carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.
- I will follow and uphold GDPR regulations.

Plashet School and the Local Authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my personal hand held/external devices (tablet/laptop/mobile telephone/USB devices etc.) in the school, I will follow the rules set out in this agreement, in the same way as if I was using school's 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.
- I will not use personal email addresses on the school ICT systems.
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will ensure that my data is regularly backed up, in accordance with relevant policies.
- 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 (unless I have permission) make large downloads or uploads that might take up Internet capacity and prevent other users from being able to carry out their work.
- 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 this is allowed in school policies.
- 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 by school policy documentation. Where personal data is transferred outside the secure LA network, it must be encrypted.
- I understand that data protection policy requires that any staff or learner 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 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 the school:

- I understand that this Acceptable Use Policy applies not only to my work and use of Plashet ICT equipment in school, but also applies to my use of school ICT systems and equipment out of the school and my use of personal equipment in the school or in situations related to my employment by London Borough of Newham.
- 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 Plashet 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/Volunteer

Name: ………………………………………………………………………….

Signed: ………………………………………………………………………….

Date: ………………………………………………………………………….

Appendix 9
Student Computer/Mobile Device User Agreement

General computer use in school

- You should expect to be supervised when using the computer rooms or using a school laptop/chromebook.
- You should not eat or drink near computers/devices. Even closed water bottles should be placed away from the devices.
- Remember to log off when you have finished.
- All devices are monitored so never use bad or inappropriate language. A screen print of any inappropriate language or sites is automatically stored.
- School devices are provided for school work only. They may not be used for leisure activities such as non-educational games.
- Manage your printer credits carefully and avoid unnecessary printing. Remember colour printing costs you more credit.
- Your user area should be well organised with all files saved in folders and all filenames should be meaningful.
- Delete any unwanted files regularly to make sure you have enough space.
- Important files should always be backed up in the cloud.
- You are not allowed to copy information from the Internet or other peoples work and claim it is your own work. This is plagiarism and is illegal under copyright law.
- Accessing someone else's computer account or any on-line account without permission is illegal under the Computer Misuse Act

Passwords and user accounts

- If you think someone else has found out your password, change it immediately.
- Make sure your password is secure. Secure passwords are not real words, are mixed case and have numbers and symbols included. Longer passwords are more secure than shorter ones.
- Do not share your user account. You could be personally responsible for anything done within your account.
- It is not good practice to have the same password for lots of accounts.

Online safety in school

- Never attempt to access any inappropriate websites.
- The use of any social networking sites or file sharing sites is banned in school.
- Remember that any on-line communication is never secure so be careful about what you say.
- You are not allowed to communicate with anyone on-line in any way unless it is part of a lesson. If it is part of a lesson your teacher will give you guidance.
- Never upload photographs to any website.
- Report anything you are worried about to a teacher.

You must agree to all of the above rules in order to log on to a school computer. By logging on you are agreeing to follow everything in the above document.

Online safety and computer use at home

- Always follow the age guidance on websites and games.
- If you are allowed to use social networking sites at home, always use the privacy settings to make your information secure.
- Do not allow 'friends' of 'friends' access to your information as you then lose control over who can see this information.
- Do not accept 'friend' requests from people you don't know.
- Remember that once you have uploaded something, you can never remove it as it may have been copied many times. Think very carefully before uploading photos.
- If you do upload a photo, make sure your location cannot be identified.
- Remove the geo-tagging information from photos as this can pinpoint where the photo was taken.
- Never include any personal contact details with photos.
- Never upload anyone else's photo without their permission, this includes group photos.
- Never meet up with anyone that you have only ever met on-line.
- Be aware that people sometimes lie about their true identity on-line.
- Never get involved in any type of cyber-bullying.
- Never spread rumours or make rude or unpleasant comments when on-line.
- Be very careful before entering personal details such as your real contact details.
- Make sure your computer system's operating system is regularly updated.
- Make sure you have anti-virus software installed and then it is regularly updated.
- There are many scams on-line, usually if it sounds too good to be true then it is too good to be true.
- Beware of phishing (being directed to a fake website that looks like the real website).
- You must not download songs, films and games unless they are from legal sources. This is considered to be theft and is a very serious crime. Most legal sources charge for downloads.
- It is very difficult to be truly anonymous on-line so bear this in mind in everything you do and say on-line.

At home you may have more freedom than at school in your computer use. Therefore, you are strongly advised to follow the above rules for your own protection and safety.

APPENDIX 10

Promoting Digital Resilience

What is Digital Resilience?

At Plashet School, the ‘Digital Resilience’ package is a suite of resources designed to safeguard young people from potentially harmful information or views presented on the Internet and through social networking sites such as YouTube, Twitter, WhatsApp, SnapChat, Instagram, Tik Tok and Facebook.

Why do we need it?

If a young person lacks the tools to make sense of their increasingly digital world, it has a direct impact on their vulnerability to potentially harmful information and agendas. The Prevent Duty: Departmental advice for schools and childcare providers (2015) states schools have a responsibility to “safeguard children and young people in England from extremists and extremist views in school and in out of school hours learning, and stop young people from becoming radicalised or acting on extreme views.'

In addition, the Common Inspection Framework (Ofsted 2015) requires learners to demonstrate an 'understanding of how to keep themselves safe from relevant risks such as abuse, sexual exploitation and extremism, including when using the internet and social media'.

Digital Resilience through the Wider School Curriculum.

In line with the school Online Safety Policy, there is an expectation for all users to promote digital resilience. This includes ensuring all e-materials used to teach the curriculum are safe for students to access and will not expose students to dangerous content. Whenever applicable, teachers and support staff should reference online safety as part of their taught curriculum content.

Digital Resilience: The taught Curriculum

Digital Resilience is taught through the Citizenship, PSHE and Computing Curriculums.

The CPSHE Curriculum

Year 8: Unit of Learning	**Digital Resilience**
1. What is the Social Networking Revolution and how has this changed the way we communicate? 2. What are the dangers of social networking? (Online grooming case-study) 3. How can I ensure I keep myself safe while online? Students are taught how to use the CEOPS ‘think you know’ website to report online activity that they deem to be a risk to their safety and well-being.	Students will describe some of the problems associated with widespread use of the internet & specifically social media. Students will apply their understanding of rights & responsibilities to explain how the dangers of internet use & specifically social networking can be mitigated through safe and responsible use of digital resources. Students will know how to report digital material that they deem to be offensive or that poses a risk to their safety and well-being. Students will begin to think about the strategy and tactics utilised by those who may wish to groom them to exploit, abuse them or groom them to commit a crime.

The Computing Curriculum

Year 7: Unit of Learning	Digital Resilience
Introduction to computing assignment ● Learn how to use the school network including the importance of good practice in using passwords. **Online safety assignment** ● CEOP videos about the dangers of meeting up with on-line contacts ● Social networking – digital footprints and privacy ● Internet use – bias, plagiarism	Students undertake an assessed piece of work within both assignments. Students will also sit a test in these units and have the opportunity to review their answers to address any misconceptions.
All Years: Responsible user agreement ● This document is discussed in the first lesson of the year. If students are seeing it for the first time the discussion is detailed. For subsequent years they are reminded about it.	The Responsible Computer User agreement has two sections. The first section is about rules and guidance within school. The second section is advice to follow outside of school.

Digital Champions and Digital Leaders

At Plashet school we recognise that almost all social media communication takes place outside of school hours, hence it is critical that students and parents are empowered with information and advice to ensure students stay safe online outside school. A key group within our student leadership programme are our 'Digital Champions' who are selected from the prefect group and work to promote an appreciation of the opportunities and risks that digital technology and social media offers. School based research and nationally recognised charities that work in the field of digital safety, all concur that messages of digital safety are far more effective when delivered by peers who students can relate to. It is also important from the perspective of keeping pace with rapidly changing technologies and applications.

The Digital Champions are the coordinators who work with the Curriculum Leader for PRE & SMSCD and the Online Safety Coordinator to lead on digital safety across all year groups. The Digital Leaders are form group representatives who work closely with individual form groups to ensure messages of digital safety are reinforced in the form group and there is a single point of contact when questions arise.

Activities undertaken by the Digital Champions include:

- receiving an annual training session from an external provider who specialises in Online Safety.
- writing a bespoke Plashet school guide called, '#dontovershare' which has been printed and distributed to all students and is also on the school website.
- delivering Online Safety assemblies to all year groups as part of Annual Safer Internet Day.
- co-designing a bespoke Plashet school Online Safety poster with the help of a professional artist.
- leading the Digital Leaders to take back messages of online safety to their individual form groups.

Appendix 11
Student Online Safety @ Plashet School

At Plashet School, we think access to the Internet is very important as it provides many educational benefits. We therefore provide Internet access in school and strongly recommend Internet access at home. We make sure that our school environment is as safe as possible. We have filtering systems in place which prevent access to certain websites. Computers and the Internet are only available for school work. In ICT, Computing and CPSHE lessons, students receive information on how to stay safe and manage online risks.

Online safety - Staying safe online, both in and out of school:

- You must be aware that someone online may be lying about their identity. If you have never met them in the real world, you have no way of knowing who they really are.
- You should never arrange to meet up with someone that you have only been in contact with online.
- Always be cautious when giving out any personal information such as your name, address, school name or phone number. Ask yourself, 'do they really need to know?'
- Always treat offers that are too good to be true with caution. You probably haven't just won an iPad or some money. They may well be after your personal information or want to spread viruses.
- Do not try to access websites that may contain offensive or inappropriate material.
- Social networking sites are banned in school. If you do use these at home, make sure you have parental permission. Understand and use the privacy settings.
- Be careful what you say online as once you have said it, you can't take it back.
- Any photos that you put up online can easily be misused without your permission, so think very carefully before posting any photos. If you do decide to post a photo, make sure names and any geo-tagging information is removed first. You must also get permission from anyone else in the photo.
- Report anything you are worried about to a responsible adult.
- Cyber-bullying (bullying using technology such as the Internet or mobile phones) is not tolerated either in or out of school.
- Ensure your passwords are secure (long, with a mix of text, numbers and characters). You should be able to remember the password but others should not be able to guess it. Do not use the same password for everything. Don't tell anyone else your password.
- It is very hard to be truly anonymous on the Internet. Therefore, you will be held accountable for anything that you do or say.
- Always make sure virus checking software is installed and updated at least every day on any computer at home. Make sure also, that your computer operating system (such as Windows) is up to date and has any security patches applied.

Plagiarism and Copyright

- You must never copy something from the Internet and pretend it is your own original work.
- You can quote from websites, but always give the source.
- When using research from the Internet, write in your own words.
- Be aware that most information, games, music, pictures and software is subject to copyright law. This means you cannot freely copy it without paying or having permission. Be aware of copyright before downloading anything.

Useful Websites

www.thinkuknow.co.uk – COEP (part of the police service)
www.nspcc.org.uk – NSPCC Child Protection
www.childline.org.uk – Childline
www.fkbko.net – For Kids by kids Online
www.iwf.org.uk – Internet Watch Foundation