PLYMSTOCK SCHOOL

E-safety Policy

Lead Officer: W M Sprenkel
Date for Review: Autumn 2021

Key Personnel

E-safety Officer: Wil Sprenkel (Deputy Headteacher)

Designated Safeguarding Lead: Wil Sprenkel (Deputy Headteacher)

Please also refer to the school's Child Protection/Safeguarding Policy and Preventing Extremism and Radicalisation Policy and Data Protection Policy (WeST)

In line with the new DFE guidance commencing 2nd September 2019. Plymstock School recognises that the use of technology has become a significant component of many safeguarding issues. Child sexual exploitation; radicalisation; sexual predation: technology often provides the platform that facilitates harm. An effective approach to online safety empowers a school to protect and educate the whole school community in their use of technology and establishes mechanisms to identify and intervene in and escalate any incident where appropriate. Plymstock's E-Safety Policy outlines how this is achieved.

Plymstock school recognises that the breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk:

• **content**: being exposed to illegal, inappropriate or harmful material; for example pornography, fake news, racist or radical and extremist views;

• **contact:** being subjected to harmful online interaction with other users; for example commercial advertising as well as adults posing as children or young adults; and

• **conduct**: personal online behaviour that increases the likelihood of, or causes, harm; for example making, sending and receiving explicit images, or online bullying.

Policy Rationale

E-safety comprises all aspects relating to children and young people and their safe use of the internet, mobile phones and other technologies, both in and out of school. It highlights the need to educate children, young people, parents, staff and all members of the school community about the benefits, risks and responsibilities of using information technology and provides safeguards and awareness for users to enable them to control their online experiences.

The Internet is an open communications channel, available to all. Applications such as the Web, e-mail, blogs and social networking all transmit information over the fibres of the Internet to many locations in the world at low cost. Anyone can send messages, discuss ideas and publish material with little restriction.

These features of the Internet make it an invaluable resource used by millions of people every day. Much of the material on the Internet is published for an adult audience and some is unsuitable for Students. Students must also learn that publishing personal information could compromise their security.

This policy applies to all members of the Plymstock School community (including staff, students, volunteers, parents / carers, visitors and community users) who have access to and are users of school ICT systems, both in and out of school.

Headteachers are empowered, to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and staff are empowered to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other E-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 E-safety behaviour that take place out of school.

Policy Statements

<u>Education – Students</u>

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in E-safety is therefore an essential part of the school's E-safety provision. Children and young people need the help and support of the school to recognise and avoid E-safety risks and build their resilience. E-safety education will be provided in the following ways:

- A planned E-safety education will be provided as part of Life Education, the assembly programme and ICT curriculum - this will cover both the use of ICT and new technologies in school and outside school.
- Students should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Students will be helped to understand the need for the Student ICT Code of Conduct and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school.
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

- Staff should act as good role models in their use of ICT, the internet and mobile devices.

Education – Parents and Carers

Many parents and carers have only a limited understanding of E-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring and regulation of the children's online experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it.

"There is a generational digital divide". (Byron Report - 2010)

The school will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters and the school website.
- E-safety communications from the DSL

Training – Staff

It is essential that all staff receive E-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- E-safety training will be provided annually to all staff.
- All new staff should receive E-safety training as part of their induction programme, ensuring that they fully understand the school E-safety Policy and Code of Conduct for ICT and general Staff Code of Conduct.
- This E-safety Policy and its updates will be presented to and discussed by staff in staff meetings.
- The E-safety Officer will provide advice / guidance / training as required to individuals as required.

Training – Governors

Governors should take part in E-safety training and awareness sessions, with particular importance for those who are members of any sub committee, group involved in ICT, E-safety, health and safety and child protection. This may be offered in a number of ways:

- Participation in school training events.
- Attendance at training provided by the National Governors Association, WeST or other relevant organisation.

Roles and Responsibilities

The following section outlines the roles and responsibilities for E-safety of individuals and groups within the school:

Governors

Governors are responsible for the approval of the E-safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors who will receive regular information about E-safety incidents and monitoring reports.

Headteacher and Senior Leaders

The Headteacher is responsible for ensuring the safety (including E-safety) of members of the school community, though the day-to-day responsibility for E-safety will be delegated to the E-safety Officer.

The Headteacher / Senior Leaders are responsible for ensuring that the E-safety Officer and other relevant staff receive suitable CPD to enable them to carry out their E-safety roles and to train other colleagues, as relevant.

The Headteacher / Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal E-safety monitoring role.

The Headteacher and E-safety Officer should be aware of the procedures to be followed in the event of a serious E-safety allegation being made against a member of staff.

E-safety Officer

Takes day-to-day responsibility for E-safety issues and has a leading role in establishing and reviewing the school E-safety policies / documents. The role includes:

- Ensures that all staff are aware of the procedures that need to be followed in the event of an E-safety incident taking place.
- Provides training and advice for staff.
- Liaises with the Local Authority, when needed.
- Liaises with school ICT technical staff.
- Receives reports of serious E-safety incidents and uses this to inform future E-safety developments.
- Review incident and filtering logs, when highlighted by the Network Manager.
- Attends relevant Governors' meeting.
- Reports regularly to Senior Leadership Team.

Network Manager

The Network Manager is responsible for ensuring:

- That the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- That users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed
- 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
- That he / she keeps up to date with E-safety technical information in order to effectively carry out their E-safety role and to inform and update others as relevant

- That the use of the network / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the E-safety Officer /Headteacher / Senior Leader / Class teacher / Head of Year for investigation / action / sanction
- That monitoring software / systems are implemented and updated as agreed in school policies

Teaching and Support Staff

Teaching and support staff are responsible for ensuring that:

- They have an up to date awareness of E-safety matters and of the current school E-safety policy and practices
- They have read, understood and signed the School Staff Code of Conduct for ICT
- They report any suspected misuse or problem to the E-safety Officer, Headteacher, Senior Leader, Class teacher, Head of Year for investigation and action
- Digital communications with students should be on a professional level and only carried out using official school systems
- E-safety issues are embedded in all aspects of the curriculum and other school activities
- Students understand and follow the school E-safety policy
- Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They monitor ICT activity in lessons, extra curricular and extended school activities
- They are aware of E-safety issues related to the use of mobile phones, media devices, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices
- 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

Designated Safeguarding Lead & Deputy Safeguarding Leads

The DSL and Deputy DSLs should be trained in E-safety issues and be aware of the potential for serious child protection issues to arise from:

- Sharing of personal data
- Access to illegal / inappropriate materials
- Inappropriate on-line contact with adults / strangers
- Sexting
- Potential or actual incidents of grooming / Child Sexual Exploitation
- Cyber-bullying

It is important to emphasise that these are child protection issues, not technical issues, simply that the technology provides additional means for child protection issues to develop.

Students

Students are responsible:

- For using the school ICT systems in accordance with the Student Code of Conduct for ICT, which they will be expected to sign before being given access to school systems.
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

- Understanding the importance of reporting abuse, misuse or access to inappropriate and/or extremist materials and know how to do so.
- Will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying.
- Should understand the importance of adopting good E-safety practice when using digital technologies out of school and realise that the school's E-safety Policy covers their actions out of school, if related to their membership of the school

Parents and Carers

Parents and 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 every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, the school website and information about national E-safety campaigns / literature.

Parents and carers will be responsible for:

- Endorsing (by signature) the Student Code of Conduct for ICT.
- Alerting the school straight away if they have any E-safety concerns or require advice/guidance.

Community Users

Community Users who access school ICT systems School will be expected to sign a Staff Code of Conduct for ICT before being provided with access to school systems.

Technical – infrastructure/equipment, filtering and monitoring

- The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably practicable and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their E-safety responsibilities:
- There will be regular checks on the safety and security of school ICT systems.
- Servers, and wireless systems must be securely located and physical access restricted.
- All users will have clearly defined access rights to school ICT systems.
- The Network Manager, who will keep an up to date record of users and their usernames, will provide all users with a username and password. Users will be requested to change their passwords regularly.
- The "administrator" passwords for the school ICT system, used by the Network Manager must also be available to the Headteacher and E-safety Officer and kept in a secure place.
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must

immediately report any suspicion or evidence that there has been a breach of security.

- The school maintains and supports the managed filtering service provided by Smoothwall. This includes filtering of key words, phrases or websites associated with extremist viewpoints.
- In the event of the Network Manager needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher or E-safety Officer.
- Any filtering issues should be reported immediately to the Network Manager.
- The Network Manager and E-safety Officer will consider requests from staff for sites to be removed from the filtered list. If the request is agreed, this action will be recorded and the E-safety Officer will review logs of such actions regularly.
- School ICT technical staff regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the Staff Code of Conduct for ICT.
- Remote management tools are used by staff to control workstations and view student activity.
- Users must report any actual / potential E-safety incident to the Network Manager or E-safety Officer.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.
- The school infrastructure and individual workstations are protected by up to date anti - virus software.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Curriculum

E-safety should be a focus in all areas of the curriculum and staff should reinforce E-safety messages in the use of ICT across the curriculum.

In lessons where internet use is pre-planned, it is best practice that 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.

Where students are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.

It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Network Manager temporarily remove those sites from the filtered list for the period of study. Any request to do so should be auditable, with clear reasons for the need.

Students should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.

Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff and students need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. Plymstock School will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.

Care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

Students must not take, use, share, publish or distribute images of others without their permission.

Photographs published on the website, or elsewhere that include students will be selected carefully.

Permission from parents or carers (through the Home-School Adgreement) will be obtained before photographs of students are published on the school website.

Students' work can only be published with the permission of the student and parents or carers.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act which states that personal data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Kept no longer than is necessary.

- Processed in accordance with the data subject's rights.
- Secure.
- Only transferred to others with adequate protection.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, USB stick or any other removable media:

- The data must be encrypted and password protected.
- The device must be password protected (many memory sticks / cards and other mobile devices cannot be password protected).
- The device must offer approved virus and malware checking software.
- The data must be securely deleted from the device once it has been transferred or its use is complete.

Communication

When using communication technologies Plymstock 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.
- All staff must adhere to the Email Protocol.
- Users must immediately report, to the Headteacher, E-safety Officer or Network Manager – 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 must be professional in tone and content. These communications should 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.
- Personal information should not be posted on the school website and only official email addresses should be used for communication.

Social Media - Protecting Professional Identity

With an increase in use of all types of social media for professional and personal purposes a policy that sets out clear guidance for staff to manage risk and behaviour online is essential. Core messages should include the protection of students, the school and the individual when publishing any material online. Expectations for teachers' professional conduct are set out in 'Teachers Standards'.

All schools, academies and local authorities have a duty of care to provide a safe learning environment for students and staff. Schools/academies and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render Plymstock School liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to students, staff and the school through limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School staff should ensure that:

- No reference should be made in social media to students / students, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the *school /academy* or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

<u>Unsuitable / inappropriate activities</u>

Some internet activity e.g. accessing child abuse images or distributing racist or extremist material is illegal is obviously banned from Plymstock School and all other technical systems.

Other activities e.g. cyber-bullying are also 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 usage as outlined on the next page.

User Actions

		Acceptable	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
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:	**Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978**				X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.				X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008				X
	criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986				X
	Pornography			X	
	Promotion of any kind of extremist viewpoints and discrimination			X	
	Threatening behaviour, including promotion of physical violence or mental harm			X	
	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			X	
Using school systems to run a private business				X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy				X	
Infringing copyright				X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)				X	
Creating or propagating computer viruses or other harmful files				X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)				X	
On-line gaming (educational)		X			
On-line gaming (non educational)				X	
On-line gambling				X	
On-line shopping / commerce			X		
File sharing			X		
Use of social media			X		
Use of messaging apps			X		
Use of video broadcasting eg Youtube			X		

E-safety incident procedures

Out-of-school cyber-bullying incident

1. HOY to investigate incident.
2. Students involved to be spoken to.
3. Parents informed.
4. Appropriate sanctions issued.
5. AHOY to provide support, advice and guidance

In-school cyber-bullying incident (involving school network or mobile devices)

1. HOY to investigate incident.
2. HOY to contact Network Manager to have network access removed of students using the school system to cyber-bully.
3. Parents informed.
4. Appropriate sanctions issued.
5. AHOY to provide support, advice and guidance.

Accessing another person's network account without permission

1. If the incident happens within a lesson the responsibility for taking action lies with the subject teacher.
2. If the incident occurs outside of lesson time the HOY will take responsibility.
3. In both circumstances the Network Manager should be contacted and network access removed for a fixed period.
4. Parents to be informed.

Accessing inappropriate/illegal/extremist material or bringing such material into school

1. If this involves the use of the school network please contact the Network Manager immediately to ensure the user account is frozen to avoid deletion.
2. Referral to the appropriate HOY who will then investigate.
3. Consult with appropriate agencies, when required (especially for illegal or extremist materials).
4. Appropriate sanctions issued (including exclusion if necessary) and network access removed for a fixed period.
5. Parents to be informed.
6. AHOY to work with student(s) so that they realise that accessing such material is not appropriate.

In the event of several E-safety incidents involving the same student(s) then referral to the E-safety officer (WMS) is appropriate.

On-line child protection / extremism / radicalisation concerns

1. Immediate referral to a Designated Safeguarding Lead in-line with safeguarding procedures.
2. DSL to coordinate response including possible Police and Social Services involvement.

Plymstock School Student Code of Conduct for ICT

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

For my own personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I will treat my username and password like my toothbrush – I will not share it, nor will I try to use any other person's username and password.
- I will be aware of the danger of talking to strangers when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line.
- If I arrange to meet people off-line that I have communicated with on-line, I will inform my parents, do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school ICT systems are intended for educational use and that I will not use the systems for personal or recreational use unless I have permission from a member of staff to do so.
- I will not try (unless I have permission from a member of staff) to 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 use the school ICT systems for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube)
- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

- I will only use my personal hand held / external devices (mobile phones / USB devices etc) in school if I have permission from a member of staff. I understand that, if I do use my own devices in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.

- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I 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 immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any attachments to emails, unless I know and trust the person / organisation who sent the email, due to the risk of the attachment containing viruses or other harmful programmes.
- 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.
- I will not use chat and social networking sites at any time in school.

When using the internet for research or recreation, I recognise that::

- I should 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 try to download copies (including music and videos).
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Code of Conduct, I will be subject to disciplinary action. This may include loss of access to the school network / internet, detentions, exclusions, contact with parents and in the event of illegal activities involvement of the police.

Students

Please complete the agreement form on the last page to show that you have read, understood and agree to the rules included in the Student Code of Conduct for ICT.

Parents

Please complete the agreement form on the next page to show that you have read, understood the rules included in the Student Code of Conduct for ICT.

Please retain the above Code of Conduct for reference – Only the agreement forms need to be returned to the school.

Parent / Carer Code of Conduct for ICT 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 technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

The attached Code of Conduct for ICT is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents and carers are aware of the importance of e-safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that students will have good access to ICT to enhance their learning and will, in return, expect the students to agree to be responsible users. A copy of the Student Code of Conduct for ICT is attached to this permission form, so that parents / carers will be aware of the school expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

Permission Form

Parent / Carers Name	
Student Name	

As the parent / carer of the above student I give permission for my son / daughter to have access to the internet and to ICT systems at school.

I know that my son / daughter has signed a Code of Conduct for ICT and has received, or will receive, e-safety education to help them understand the importance of safe use of ICT – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's / daughter's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Code of Conduct.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's e-safety.

Signed…… Date……

Student Code of Conduct Agreement Form

Please complete the sections below to show that you have read, understood and agree to the rules included in the Code of Conduct.

If you do not sign and return this agreement, access to the school ICT systems will be removed.

I have read and understand the above and agree to follow these guidelines when:

- I use the school ICT systems and equipment (both in and out of school)
- I use my own equipment in school (when allowed) e.g. iPads, tablets, laptops, cameras etc…
- I use my own equipment out of school in a way that is related to me being a member of this school e.g. communicating with other members of the school, accessing school email, the intranet, website etc…

Signature……

Print name……..

Tutor group…….

Year group……..

Date…….

Plymstock School Staff (and Volunteer)
Code of Conduct for ICT

To ensure that you are fully aware of your professional responsibilities when using information systems and when communicating with pupils, you are asked to sign this code of conduct.

Members of staff should consult the school's E-safety policy for further information and clarification.

- I understand that it is a criminal offence to use the school ICT system for a purpose not permitted by the Headteacher.
- I appreciate that ICT includes a wide range of systems, including smart phones, iPads, digital cameras, email, social networking and that ICT use may also include personal ICT devices when used for school business.
- I understand that school information systems may not be used for private purposes without specific permission from the Headteacher.
- I understand that my use of school information systems, Internet and email will be monitored and recorded to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager.
- I will ensure that personal data is stored securely and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the E-Safety Oficer, a Child Protection Officer or Headteacher.
- I will ensure that electronic communications with students and parents are completed using school systems and that they are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
- I will promote E-safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.
- When I use my personal hand held / external devices (PDAs / laptops / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the school ICT systems apart from specifically designated times.
- 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 not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, extremist material and adult pornography covered by the Obscene Publications Act) or material that is inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.

- I will not try (unless I have permission from the Network Manager) to 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 has been authorised by the Network Manager.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others in the school. Where personal data is transferred outside the secure school network, secure SIMs access or other secure method, it must be encrypted.
- I understand that data protection policy requires that any staff or student data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- Any loss of personal or confidential information must be reported immediately to the E-Saftety Officer.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will adhere at all times to the schools Email Protocol.

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 that may have converted from sites such as YouTube).

I understand that I am responsible for my actions in and out of school:

- I understand that this Code of Conduct for ICT applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and / or the Local Authority and in the event of illegal activities the involvement of the police.

The school may exercise its right to monitor the use of the school's information systems and Internet access, to intercept e-mail and to delete inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood and accept the Staff Code of Conduct for ICT.

Signed: …… Capitals: ……... Date: ……..

Policy History

Policy / Version Date	Summary of change	Contact	Implementation Date	Review Date
Autumn 2017	Policy review	Deputy Headteacher Pastoral	September 2019	Annual Review