Pield Heath House School

e-Safety Policy

(Including Use of VDU's and Ergonomics)

Reviewed: September 2020
Next Planned Review: September 2021

Acceptable Use of the Internet and Related Technologies

Contents:

This e-Safety Policy has been written by the school, building on the London Grid for Learning (LGfL) and Becta policy guidance. It has been agreed by the Senior Leadership Team and approved by Governors. It will be reviewed bi-annually or sooner if required. The policy will be monitored by the e-Safety Officer in conjunction with the Pastoral Care Team and Designated (Safeguarding) Lead. The e-Safety Policy forms part of the School Development Plan and relates to other policies including:

- Anti-bullying Policy
- Safeguarding Policy
- Pastoral Care Policy
- Data Protection Policy
- Use of Digital Images Policy

This policy also includes the guidance on VDU's which has been included in order to comply with the **Health and Safety {Display Screen Equipment} Regulations 1992 and Computer Misuse Act 1990.** These regulations apply not only to conventional VDU's but also to non-electric systems. In short, most screen equipment which displays text, numbers or graphics is covered by the regulations **{DSE = Display Screen Equipment}.** The regulations require employers to take certain measures to protect the health and safety of DSE users. A DSE user is signified as someone who 'habitually uses DSE as a significant part of their normal work', significant being an hour or more on most working days.

This document will provide protocols for the effective and legal use of all IT Equipment. This policy is mandatory and staff who fail to observe the protocols laid out within the document may render themselves liable to disciplinary action, up to and including dismissal. It should be noted that the use of a computer system without permission or for a purpose not agreed by the school, could constitute a criminal offence under the **Computer Misuse Act 1990.**

Pield Heath House School
e-Safety Policy and Procedures

1. Introduction

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

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

- The Internet
- e-mail
- Instant messaging (msn / aol /bbm)
- web cams
- Blogs (an on-line interactive diary)
- Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player)
- Social networking sites (myspace / piczo/ bebo)
- Video broadcasting sites (youtube.com/ Instagram/tiktok)
- Chat Rooms (teenchat / habbohotel)
- Gaming Sites (neopets/miniclip/runescape)
- Music download sites (apple/itunes/ napster / kazzaa.com/ livewire)
- Mobile phones with camera and video functionality
- Smart phones with e-mail, web functionality and cut down 'Office' applications.

Whilst exciting and beneficial both in and out of the context of education, much Technology and Internet use, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

At Pield Heath House School we have a responsibility to educate our pupils in e-Safety issues such as;

- Teaching them the appropriate behaviours and thinking skills to enable them to remain safe and
- Remain legal when using the internet and related technologies, in and beyond the context of the classroom.

In order to achieve this, we will ensure that:

- Internet access will be planned to enrich and extend learning as part of the national curriculum.
- Students will be given clear guidelines for Internet use and a list of suitable websites.
- Students will be educated in safe Internet use and the dangers to be aware of.
- Students will only be allowed to access the internet following specific authorisation from parents/carers.
- Student access to the internet will be closely supervised at all times.
- Students must not print pages from the internet unless authorised to do so.
- Curriculum Internet use will be planned, task-orientated and educational.

This policy is inclusive of both fixed and mobile internet; technologies provided by the school; (such as PCs, laptops, tablets, webcams, whiteboards, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, iPads, mobiles phones, camera phones and portable media players, etc).

Personal Use of IT

IT facilities are provided throughout the school to assist staff in fulfilling their duties and to enable the school to meet its operational and strategic objectives. However limited personal use is permitted provided there is no cost to the school through such use. Any personal use is only permitted provided the following guidelines are adhered to:

- Internet use for personal use must be in your own time
- It should not involve large downloads
- Such use should not be for personal financial gain, gambling, political purposes or personal advertising.

Security of the School IT System and VDU Equipment

- It is essential that IT facilities are at all times used in a professional manner as failure to do so could result in legal liability.
- Staff and in turn students will be given clear guidelines and objectives for Internet use.
- Internet access will be available for students in the school.
- Students will only be permitted to access the Internet under constant supervision.
- Personal data sent over the Internet will be encrypted or otherwise secured.
- Students will be given guidance on the safe use of computers and the Internet.
- To gain knowledge of e-mail, students will be issued with an e-mail address and they can send e-mails internally. Alternatively, parentally verified e-mail addresses of family can also be used.
- Random checks of e-mail accounts will be carried out by staff to ensure undesirable literature does not filter through.
- Personal floppy disks/CD's/Memory Sticks may not be used on the school's IT system without prior permission and running a virus scan
- When copying materials from the Web, copyright will be observed by all.
- Only students who have parental permission will be allowed to have Internet access.

2. Whole School Approach to the Safe Use of Technology and Internet

Creating a safe online learning environment includes three main elements at this school:

- An effective range of technological tools;
- Policies and procedures, with clear roles and responsibilities;
- A comprehensive e-Safety education programme for pupils, staff and parents.

3. Roles and Responsibilities

As e-Safety is an important aspect of strategic leadership within the school, the Executive Principal and Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named e-Safety Officer will be **Louise Mahon**

Our e-Safety Officer will ensure that she keeps up to date with e-Safety issues and guidance through liaison with the Local Authority e-Safety Officer and through other organisations such as Becta, London Grid for Learning and The Child Exploitation and Online Protection (CEOP)

i) The school's e-Safety Officer will ensure that the Executive Principal, SLT and Governors are updated as necessary. Governors need to have an understanding of e-Safety issues and strategies that are in place.

ii) We ensure our governors are aware of local and national guidance on e-Safety and are updated at least annually on policy developments.

iii) The Pastoral Care Team will audit this policy requirement annually; ensuring signed agreements are in place for staff and students.

All teachers are responsible for promoting and supporting safe behaviours in their classrooms and following the schools' e-Safety procedures. Central to this is fostering a 'Telling School' culture so pupils feel able to report any bullying, abuse or inappropriate materials.

All staff will be fully aware of the schools' e-Safety Policy including:

- Safe use of e-mail;
- Safe use of Internet including use of internet based communication services, such as instant messaging and social network;
- Safe use of school network, equipment and data;
- Safe use of digital images and digital technologies, such as mobile phones and digital cameras;
- Publication of pupil information/photographs and use of website;
- e-Bullying / Cyber bullying procedures
- Their role in providing e- Safety education for pupils;

All Staff (all teachers, SSA's, agency staff and associate staff) are reminded / updated about e-Safety matters at least once a year.

4. Handling E-Safety Risks, Concerns and Complaints

There are many risks associated with E-Safety which are primarily caused by people acting inappropriately. A potential issue must be dealt with immediately, with the Tutor being the first line of defence. A Tutors observation of a student's behaviour is essential in detecting potential danger to students. It is therefore the Tutors responsibility to immediately report any incidents of concern. Issues of concern can vary from pranks and unconsidered activities to considered illegal activity. The following points will help staff determine level of concern and action required.

What are electronic communication systems?

- Internet collaboration tools (social networking sites/web logs (blogs))
- Internet research (websites/search engines/web browsers)
- Mobile phones & personal digital assistants (PDAs)
- Internet communication (e-mail/IM)
- Webcams and videoconferencing
- Wireless games consoles.

What are the risks?

- Receiving inappropriate content
- Predation and grooming
- Requests for personal information
- Viewing 'incitement' sites
- Bullying and threats
- Identity theft
- Online gambling
- Misuse of computer system
- Publishing personal information
- Hacking and other security breaches
- Corruption or misuse of data

Response to incidents of concern

The school will take all reasonably practicable precautions to ensure e-Safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.

5. Safety and the Internet

Available from Becta, the Government agency at:

http://schools.becta.org.uk and http://www.ceop.gov.uk

Staff and pupils are given information about infringements in use and possible sanctions.

Sanctions include:

- Discussion with e-Safety Officer / Executive Principal;
- Informing parents or carers;
- Removal of Internet or computer access for a period, [which could ultimately prevent access to files held on the system];
- Referral to Police.

The e-Safety Officer will be the first point of contact for complaints. Any complaint about staff misuse is referred to the Executive Principal. Any complaint about the Executive Principal misuse will be referred to the Chair of Governors.

Complaints of cyber bullying are dealt with in accordance with our Anti-Bullying Policy.

Complaints related to child protection are dealt with in accordance with school / LA Safeguarding Procedures

To enhance learning through computing the school will;

- Provide opportunities within a range of curriculum areas to teach e-Safety.
- Educate pupils on the dangers of technologies that may be encountered outside school, ensuring it is done so informally when opportunities arise and as part of the e-Safety curriculum.
- Ensure pupils are aware of the impact of online bullying and know how to seek help if these issues affect them. Pupils are also made aware of where to seek advice or help if they experience problems when using the Internet and related technologies; i.e. parent/carer, teacher/trusted member of staff, or an organisation such as Childline/CEOP.
- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear guidelines for Internet use.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Education programme

At Pield Heath School we:

- Foster a 'Telling School' culture that encourages pupils to tell a teacher / responsible adult immediately if they encounter any material that makes them feel uncomfortable;
- Ensure pupils and staff know what to do if they find inappropriate web material i.e. to switch off monitor and report the URL to the teacher or e-Safety Officer
- Ensure pupils are taught how to evaluate Internet content and to be critically aware of the materials they read and are shown how to validate information before accepting its accuracy.
- Deliver E-safety education from Key Stage 2 at an age appropriate level
- Ensure pupils and staff know what to do if cyber-bullying or other e-safety incidents occurs;

Managing Internet Access

1. Information system security

This school:

- Ensures virus protection will be updated regularly.
- Use class/individual login as appropriate
- We use a filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature; Staff and students are instructed that that they must report any failure of the filtering systems directly to the e-Safety Officer/IT Co-ordinator who then informs system administrator. Our systems administrators report to the Executive Principal where necessary.
- Blocks all Chat rooms and social networking sites except those that are part of an educational network or an approved learning platform;
- Only uses approved blogging or discussion sites, such as on the LGfL etc
- Only uses approved or checked webcam sites;

2. Authorising Internet access

EMAIL

- Pupils may be introduced to, and use e-mail as part of their cross curricular work.
- Staff can use the school domain e-mail accounts or web-based email for professional purposes or for uses deemed 'reasonable' by the Executive Principal and Governing Body.

IMAGES

- Digital images /video of pupils are stored in the teachers' shared images folder on the network and images are archived in line with Data Protection at the end of the year – unless an item is specifically kept for a key school publication;
- We do not use pupils' full names when saving images in the file names
- We do not include the full names of pupils in the credits of any published school produced video materials / DVDs;
- Staff sign the school's E-Safety (formerly VDU & Internet Safety Policy) which includes a clause on the use of mobile phones / personal equipment for taking pictures of pupils;
- Pupils are taught to publish for a wide range of audiences which might include governors, parents or younger children as part of their online education.

- Pupils are taught about how images can be abused in their E-Safety education programme;

USING THE NETWORK AND EQUIPMENT

This school:

- Ensures staff are set-up with Internet and email access and are given an individual network log-in username and password;
- Provides pupils with a class network log-in username;
- Makes it clear that staff must keep their log-in username and password private and must not leave them where others can find;
- Makes clear that pupils should never be allowed to log-on or use teacher and staff logins – these have far less security restrictions and inappropriate use could damage files or the network;
- Makes clear that no one should log on as another user – if two people log on at the same time this may corrupt personal files and profiles; they are also informed of the possible legal implications of allowing another person to log on with their details;
- Has set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas;
- Requires all users to always log off when they have finished working or are leaving the computer unattended;
- Has a 'time-out' system in place which ensures a computer 'goes to sleep' after a specified length of time being idle. Where a user finds a logged-on machine, we require them to always log-off and then log-on again as themselves;
- Requests that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used solely to support their professional responsibilities and that they notify the school of any "significant personal use" as defined by HM Revenue & Customs.

Handling Infringements

Whenever a student or staff member infringes the e-Safety Policy, the final decision on the level of sanction will be at the discretion of the Executive Principal or at the discretion of the Governors in the case of the Executive Principal.

The following are provided as exemplification only:

Students

Category A infringements:

- Use of non-educational sites during lessons
- Unauthorised use of email
- Unauthorised use of mobile phone (or other new technologies s) in lessons e.g. to send texts to friends
- Use of unauthorised instant messaging / social networking sites

Category A Sanctions:

- Referred to class teacher
- Referred to SLT if deemed serious or child protection issue

Category B infringements:

- Continued use of non-educational sites during lessons after being warned
- Continued unauthorised use of email after being warned

- Continued unauthorised use of mobile phone etc. after being warned
- Continued use of unauthorised sites such as instant messaging / chatrooms, social networking sites.
- Use of Filesharing software e.g. Napster, Vanbasco, BitTorrent, LiveWire, etc
- Accidentally corrupting or destroying others' data without notifying a member of staff
- Accidentally accessing offensive material and not logging off or notifying a member of staff of it
-

Category B Sanctions

- Referred to class teacher, senior teacher and e-Safety Officer. Next steps/consequences agreed by both.
- Parents informed.

Category C infringements:

- Deliberately corrupting or destroying someone's data, violating privacy of others
- Sending an email or MSN message that is regarded as harassment/ bullying
- Deliberately trying to access offensive or pornographic material
- Any purchasing or ordering of items over the Internet
- Transmission of commercial or advertising material

Category C Sanctions:

- Referred to class teacher, Associate Head and e-Safety Officer. Next steps/consequences agreed by both.
- If deemed more serious, in consultation with Executive Principal/Associate Heads/Class Tutors
- Parents informed.
- Removal of Internet access rights for a period.
- Removal of equipment if applicable.
- If inappropriate web material is accessed:
- Ensure appropriate technical support filters the site.

Category D infringements:

- Continued sending of emails or MSN messages regarded as harassment or of a bullying nature after being warned
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1998
- Bringing the school name into disrepute

Category D Sanctions:

- Referred to class teacher, Associate Head and e-Safety Officer. Next steps/consequences agreed by both.
- If deemed more serious, in consultation with Executive principal
- Parents informed.
- Removal of Internet access rights for a period.
- Removal of equipment if applicable.
- Refer to LA e-Safety officer and/or Community Police Officer if deemed necessary

Other safeguarding actions:

- Secure and preserve any evidence
- Inform the sender's e-mail service provider

Staff

Category A infringements (Misconduct):

- Excessive use of Internet for personal activities not related to professional development e.g. online shopping, personal email, instant messaging etc.
- Misuse of first level data security, e.g. wrongful use of passwords
- Breaching copyright or license e.g. installing unlicensed software on network

Category A Sanctions:

- Referred to Line Manager and e-Safety officer.
- If deemed more serious, referred to Executive principal and warning given.

Category B infringements (Gross Misconduct):

- Serious misuse of, or deliberate damage to, any school computer hardware or software;
- Any deliberate attempt to breach data protection or computer security rules;
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent;
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988;
- Bringing the school name into disrepute.

Category B Sanctions:

- Referred to Executive Principal
- Governors informed and advised to follow school disciplinary procedures.
- Report to Police if appropriate.

Other safeguarding actions:

- Remove the PC to a secure place to ensure that there is no further access to the PC or laptop.
- Instigate an audit of all IT equipment by an outside agency, to ensure there is no risk of pupils accessing inappropriate materials in the school.
- Identify the precise details of the material.

If a member of staff commits an exceptionally serious act of gross misconduct they should be instantly suspended. Normally though, there will be an investigation before disciplinary action is taken for any alleged offence. As part of that the member of staff will be asked to explain their actions and these will be considered before any disciplinary action is taken.

In the case of Child Pornography being found, the member of staff will be immediately suspended and the Police will be called.

Anyone may report inappropriate or potentially illegal activity or abuse with or towards a child online to:

Police on 0808 100 00 40 or **www.met.police.uk/child pornography**

Child Exploitation and Online Protection (CEOP) at www.ceop.gov.uk/reporting_abuse

Informing staff and students of our procedures.

- The procedures will be fully explained and included within the school's e-Safety / Acceptable Use Policy. All staff will be required to sign the school's e-Safety Policy acceptance form;

- Pupils will be taught about responsible and acceptable use and given strategies to deal with incidents so they can develop 'safe behaviours'. Pupils will sign an age appropriate e-Safety / acceptable use form; (This is also produced in symbol format)
- The school's e-safety policy will be made available and explained to parents, who also sign a permission form authorising their child to have Internet access; these forms are kept in the school office in the students file.
- Information on reporting abuse / bullying etc. will be made available by the school for pupils, staff and parents.

Ergonomic Health & Safety

Each VDU user is responsible for the risk assessment of their workstation. The completed assessment should be passed to the Health and Safety Officer for action/filing.

DSE Ergonomics.

The following is a list of recommended practices for DSE users. It is in the users' best interest to follow them.

- Users should be able to make adjustments to equipment to suit him/her self (i.e. chair height, screen position etc)
- Furniture should be adjustable for height and angle so that the small of the back is supported.
- Thighs and arms should each be level.
- Use footrest where necessary to acquire correct leg height adjustment
- Wrists should rest on desk and elbows and should not stick out, particularly when using the mouse.
- Desk should be designed so as not to restrict chair adjustments
- Room should be arranged so as to avoid craning of the neck.
- Screen should be free from finger marks, dirt and grim.
- Situate screen so as to avoid glare from light or sun.
- The maximum time of continuous use of DSE should not exceed ***90 minutes***.
- A break of 5 minutes should be taken in every 30 minutes
- Damaged IT equipment must be reported immediately via the IT Repair/Request Book located in reception.
- Damaged workstation equipment and other DSC equipment must be reported immediately on a Fault Report Sheet and where applicable mark as 'Out of Order' or 'Do Not Use' to ensure safety of others.

Web Links:

- Safeguarding Children in a Digital World (Ref: BEC1-15401)
- E-Safety (revised) (Ref: BEC1-15402)
- Signposts to Safety (Ref: BEC1-15274 (KS3 & KS4))

Associated Legal Framework

- Racial and Religious Hatred Act 2006
- Sexual Offences Act 2003
- Communications Act 2003 (section 127)
- Data Protection Act 1998
- Computer Misuse Act 1990 (section 1-3)
- Malicious Communications Act 1988 (section 1)
- Copyright, Design and Patents Act 1988
- Public Order Act 1986 (section 17-29)
- Protection of Children Act 1978 (section 1)
- Obscene Publications Act 1959 & 1964
- Protection from Harassment Act 1997
- Regulation of Investigatory Powers Act 2000.

Reference Material:

- DCSF Guidelines
- Work with Display Screen Equipment, HSE Guidance and Regulations
- www.clusterweb.org.uk?esafety

STAFF E-SAFETY AND VDU CODE OF CONDUCT AND AGREEMENT.

I the undersigned agree that I am fully aware of my professional responsibilities when using the Computing and VDU facilities available to me at Pield Heath House School.

I understand that Computing and VDU includes a wide range of systems, including Laptops, iPads, mobile phones, PDA's, digital cameras, email, IM, social networking and that Computing also includes personal IT devices such as mobile phones, tablets & cameras when used for school business.

I understand that my use of the school information systems, the Internet and e-mail will be monitored and recorded to ensure policy compliance.

I will respect system security and I will not disclose my password or login details to anyone other than the authorised system administrator. I also understand that I am responsible for all activities carried out under my username even if such activities result in legal liability.

I agree that in the event I need to take school Computing or VDU equipment off site, including to my home I will first complete the appropriate request form listing the item I need to remove, the purpose for which I require it and the length of time I expect to have it. This will be passed to my line manager for authorisation. I understand I am solely responsible for this equipment whilst it is in my possession and I must be fully aware at all times of it whereabouts. I also understand that I may be legally liable for any inappropriate use of this equipment during this time.

I will ensure that students personal data is stored securely and is used appropriately, whether in school or taken off the school premises. I understand that I am only authorised to remove personal data on encrypted devices. I also understand that I must not use my personal equipment i.e. mobile phone/tablet etc to take or store images or personal information about a student or students.

I will not establish or seek to establish social contact with students for the purpose of securing a friendship or to pursue or strengthen a relationship. This extends to the use of social networking sites such as facebook, text messages and e-mail. I will not 'friend' a student present or past or their families on any social networking site such as facebook. If I use facebook as a part of a program of education I will set up groups or pages to do this (see facebook's guide on this at http://facebookforeducators.org/)

I will respect copyright and intellectual property rights at all times.

I will promote e-safety with the students in my care and will help them to develop a responsible attitude to the use of technology and the internet.

I will report any incidents of concern regarding students' safety to the E-Safety Officer and School Principal.

Signed:	**Print Name:**
Position:	**Date:**
Witness Signature:	**Date:**

STUDENT INTERNET USE ACCEPTANCE AGREEMENT

Pield Heath House School now have computers with Internet Access. The steps set out below will help to keep you safe when using the Internet.

School Agreement

In order to meet your educational and social need to gain computer literacy, we will:

- provide computers with Internet Access for your use
- ensure these computers are regularly serviced and maintained to keep them safe for use.
- give you training on how to use computers and access the Internet safely
- supervise and monitor all computer use by students
- install and regularly update virus protection and other related software
- install Firewall and Spam guard
- activate 'Parental controls' to ensure only appropriate sites are accessed

Student Agreement

- I will always gain permission before using a computer and accessing the Internet
- I understand I can only use a computer and access the Internet under supervision
- I will use the computers and the Internet for schoolwork only
- I will not access other peoples files
- I will only access Internet sites that are appropriate to my schoolwork and have my teachers approval
- I will only e-mail people my teacher has approved of
- The messages I send through e-mail will be polite and responsible
- I will never give my home address or telephone numbers to anyone
- I will report any unpleasant material or messages I receive from inside or outside the school

Student Agreement	
Student Name: (Print)	**Student Signature:**
Tutor Group:	**Date:**
Signed on behalf of Pield Heath House School:	**Date:**

Pield Heath House School
e-Safety Policy and Procedures

Pield Heath Road
Uxbridge
Middlesex UB8 3NW
Telephone: 01895 258507
Fax: 01895 256497
email:admin@pieldheathschool.org.uk

Dear Parent/Carer,

As part of the students' curriculum enhancement and the development of their technology and internet skills, Pield Heath House School is now providing supervised access to the Internet, in the classrooms and the IT suite. Students will be able to gather information from a given list of suitable websites which will include access to museums, libraries and news providers. Students will be able to exchange electronic mail (e-mail) internally or externally to a parentally verified e-mail address of a family member.

Although there may be concerns about students having access to undesirable materials on the internet, we continuously take proactive steps to reduce the risk of this happening to its lowest possible level. These measures include:

- **Firewall:**
  -prevents malicious attacks
  - restricts access to inappropriate sites which can be accessed through entering a word into a search engine e.g. Middlesex could link to an inappropriate site because of 'sex' in the word Middlesex.
- **Cyber sitter:**
  -prohibits links to inappropriate sites flashing up as advertisements on any webpage.
  -blocks access to Instant Messaging sites and social networking sites (chat rooms)

Should you wish to discuss any aspect of our E-Safety Policy, please feel free to contact in the first instance our e-Safety Officer.

Yours sincerely

Sr. Julie Rose.

_____

Parental/Carer Agreement

I do/do not give permission for my child _____ to use the internet in school for learning as part of their curriculum studies.

Signed: _____ **Date**: _____