The Purbeck School

Achieving Excellence Together

Name of policy	E-SAFETY POLICY
Date first adopted	July 2014
How often to be reviewed	Annually
Reviewed	December 2018
Reviewed	January 2019
Reviewed	24th March 2021
Governor Committee	Student Development

Name of policy: E Safety Policy

Designated Safeguarding Lead: Louise Robinson, Assistant Headteacher

Named Governor with lead responsibility: Anna Daniels

Date first adopted: July 2014

Date reviewed and updated: January 2021

Date agreed and ratified by Governing Body:

Date of next review: March 2022

Section 1: E–safety vision

As a community school we are dedicated to providing a safe environment for our students, where are our students show respect, aspiration and perseverance. We embrace the Internet and mobile technology as fantastic tools in our learning; our aim is to make sure students get the best use from it by educating them how to use it safely and responsibly. The Purbeck School recognises that clear E-Safety guidance and planning will help to ensure appropriate, effective and safer use of electronic communications for use in school, recreational and personal use for all within our community.

Section 2: Roles and Responsibilities

The following section outlines the e-safety roles and responsibilities of individuals and groups within The Purbeck School.

The Purbeck School recognises that all members of the community have important roles and responsibilities to play with regards to online safety.

E–Safety Group

The E-Safety Group provides a consultative group that has wide representation from the school community with responsibility for issues regarding e-safety and the monitoring of the e-safety policy, including the impact of initiatives. The group will also be responsible for regular reporting to the Governing Body. All stakeholders will be actively involved in the group and will have an impact on ensuring that policies are understood and implemented. The governing body will formally approve the E-safety policy.

Name	Role	RESPONSIBILITY
V Gregory	SLT & DSL	Child protection
M Lawson	Deputy DSL	Child protection/Training for staff and students
J Lay	Head of IT	Curriculum
A Humphreys (AHS)	Head of PHSE	Awareness/curriculum
J Deremaux L Robinson T Mockridge N Hunt	House Leaders	Awareness, student support/education
A Daniels	CP / Parent Governor	
School council		Collaborative work

Section 3: Policy scope

The e-safety policy covers the use of the computing systems, equipment and software in school. It also covers the use of school-owned technology outside of school and the use of personal technology in school. It is comprehensive in that it includes sections on issues such as social networking, cyber- bullying, data protection, passwords, filtering, digital and video images and use of mobile and / or gaming devices. The policy clearly states the school's commitment to act on e-safety incidents outside the school that affect the wellbeing of staff and students.

Whole school e-safety will be embedded in all relevant whole school policies (behaviour, anti-bullying, PSHE, child protection, safeguarding and computing/ICT). As a school we have carefully considered our approach to e-safety and communicate a consistent e-safety message to all members of our community, through a variety of media and activities that promote whole school input.

Section 4: Policy Aims

The purpose of systems in place is to safeguard our students while providing guidance on current e-safety issues such as cyber-bullying, youth produced sexual imagery (sexting), grooming and pornography to both students and parents. Staff and governors will be provided with e-safety awareness training so that they are aware of their responsibilities and of current e-safety issues.

Students are responsible for using the school ICT systems in accordance with the Student Acceptable Use Policy (AUP), which they will be expected to sign before being given access to school systems.

- They will have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- They need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- They 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.
- They 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.

Section 5: Vulnerable students

The Purbeck recognises that some learners are more vulnerable online due to a range of factors. This may include, but is not limited to children in care, children with disabilities and Special Educational Needs and (DSEN) or mental health needs and children experiencing trauma or loss.

Staff are made aware (through the child protection policy, the anti-bullying policy and regular training) of this increased vulnerability. This information is also kept in mind when reviewing the regular filtering reports. Through tutor times, assemblies and supportive educational discussion, students will be educated about the risks and vulnerabilities posed by electronic media.

Section 6: Online Sexual Violence and Sexual Harassment between Children

Our setting has accessed and understood "Sexual violence and sexual harassment between children in schools and colleges" (2018) guidance and part 5 of 'Keeping children safe in education' 2018.

The Purbeck School recognises that sexual violence and sexual harassment between children can take place online. Examples may include; non-consensual sharing of sexual images and videos, sexualised online bullying, online coercion and threats, unwanted sexual comments and messages on social media, and online sexual exploitation.

Full details of how we will respond to concerns relating to sexual violence and sexual harassment between children can be found within our child protection and anti-bullying policy. See also Appendix A.

Section 7: Incidents of youth produced sexual imagery (previously known as "Sexting"):

The Purbeck School will follow the advice as set out in the non-statutory UKCCIS guidance: 'Sexting in schools and colleges: responding to incidents and safeguarding young people'.

Youth produced sexual imagery involves the exchange of sexual messages or self-generated sexual images or videos through a mobile phone network or the internet.

Youth refers to any young person under the age of 18.

Once a message or image has been shared, the sender has no control about how it is used. It can leave a child vulnerable to bullying, blackmail, online grooming or abuse. It is a criminal offence to create or share explicit images of a youth, even if the person doing so is a child/youth.

Incidents of youth produced sexual imagery must be dealt with in-line with child protection procedures. Please see reporting procedure for further information (Appendix A) and refer to The Purbeck School's Child Protection Policy.

Devices, believed to contain youth produced sexual imagery, will be confiscated and must be given to the DSL (or deputy DSL). Try to avoid looking at the image. If it is necessary to look at the image, this will only be done by the DSL (or Deputy DSL). Do not take copies and do not forward to anyone. Devices will be locked away until decisions have been made. If there is no Police involvement, the image will be deleted and the device will be returned. If Police are involved the device will be retained and handed to the police.

If a student refuses to hand over a device, the school may well have to involve the police in line with child protection policies.

Generally, if the issue occurs during the school day, during an off-site activity/trip or during travel to/from school, then school will investigate. If the issue occurs outside of school, then the school will provide support.

If the issue occurs outside of school, but involves any content recorded during school related activity, then the school will investigate. Any issue aimed at staff, the school, or the reputation of the school will be investigated regardless of when it occurs. Please refer to the behaviour policy, anti-bullying policy and child protection policy for further guidance and information.

Section 8: Online Radicalisation and Extremism

We will take all reasonable precautions to ensure that students and staff are safe from terrorist and extremist material when accessing the internet on site.

If we are concerned that a student or parent/carer may be at risk of radicalisation online, the DSL (or deputy DSL) will be informed immediately, and action will be taken in line with the school's child protection policy.

If we are concerned that member of staff may be at risk of radicalisation online, the Headteacher will be informed immediately and action will be taken in line with the child protection and allegations policies.

The implementation of this e-safety policy will be monitored by the :	*Assistant Headteacher & DSL*
Monitoring will take place at regular intervals :	Internal review annually Review by Governors committee – Every 2 years
The Governing Body / Student development group(SDG) will receive a report on the implementation of the e-safety policy generated by the E-safety group (which will include anonymous details of e-safety incidents) at regular intervals:	Termly meetings
The E-Safety Policy will be reviewed formally every 2 years, or more regularly in light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next Anticipated review date will be :	Autumn term 2022
Should serious e-safety incidents take place, the following external persons / agencies should be informed :	*LA, SwGFL, CHAD*

Section 9: Acceptable Use Agreements

The Acceptable Use agreement will be provided to parents and carers as part of the new 'Student Induction Pack'. The school will ask all new parents to sign the ICT user agreement when their child starts with the school. Parents will be offered e-safety training and updates.

When logging on to the school network, year 7 to 11 students have to accept the AUP (Acceptable Use Policy) for every log on. Sixth form students accept the AUP at the start of every half term. Students need to agree to comply with the student AUP in order to gain access to the school IT systems and to the Internet.

The School's induction process and practice guarantees that adults who are new to the school are informed of and required to acknowledge (or sign) Acceptable Use Agreements. All staff will be shown where to access the e-safety policy and its importance explained. All staff are required to accept the AUP the first time they log in to a school computer, and then annually at the start of the Autumn term. All staff will receive e-safety training on a regular basis.

Annually, the Schools network requires staff to respond to a dialogue box and acknowledge the AUP. All staff must sign and agree to comply with the staff AUP in order to gain access to the school IT systems and to the internet.

Section 10: Sanctions

Sanctions for e- safety abuse or misuse will be in line with the school behaviour policy. Staff are aware of sanctions and understand their importance. Users understand that sanctions can be applied to e-safety incidents that take place out of school, if they are related to school (e.g. cyber bullying); this will be at the discretion of the school.

Section 11: Reporting

Users will be made aware of the school reporting systems. It is everyone's duty to ensure that incidents are reported. We have a clear process for logging e-safety incidents that safeguard our students from e-safety issues.

The School's website has a CEOP online reporting button that allows students to report e-safety incidents. All e-safety incidents will be reported to the School Development Group (SDG).

Please see reporting procedure for further information (Appendix A).

Cyber-bullying

The Purbeck School actively encourages the entire school community to be vigilant about the risks posed by mobile and wireless technology through its e-safety education programme for students, staff, governors and parents.

The school recognises its inability, beyond the comparative safety of the School's ICT network, to control the actions of its students in cyberspace. However, the School's behaviour and anti-bullying policies apply equally to cyber-bullying. The Purbeck School will provide an online anonymous reporting mechanism to enable students to report any incidents or concerns. This will be available through the school website.

Section 12: Communications Technologies

Mobile Devices

Use of personal electronic devices in school is allowed at KS5 (sixth form) to support teaching and learning. Other key stages are not allowed use of mobile devices in school.

Mobile phones must be switched off and out of sight once students arrive on the school site. Mobile phones may only then be used at the end of the school day. Substantial research indicates that mobile phones (in particular when used to access social media) can have a detrimental impact on young people's mental health.

Should parents and carers need to get in touch with their child then communication must take place via the school office. If a student needs to contact home they must do so via 'Reception'.

The school's approach to managing the widespread student ownership of these devices will be reviewed regularly.

Any electronic devices brought to school are the responsibility of the owner; the Purbeck School accepts no responsibility for loss, theft or damage to such items.

The School's wireless network will be available to students at KS5 (sixth form) for mobile use, and will be filtered according to age. The school has several levels of filtering for Internet access.

The use of mobile technology to send abusive or inappropriate text messages or email is forbidden, as is the videoing or photographing of others without permission. The School recognise the importance of parents/ carers role in being aware of students' online usage at home. The school website is used to promote and support parents/carers by providing informative material and guidance to various website such as the NSPCC. Please reference the Purbeck School behaviour policy for further details of appropriate use of mobile devices and how inappropriate use will be sanctioned.

Social Media

Access to social networking sites, such as Facebook, Twitter and chat-rooms, will either be blocked or access will be filtered. Newsgroups will be blocked, unless a specific use is approved.

YouTube will be available for students and staff but will be filtered for access to educational material only; filtering will also be age appropriate. Staff may seek permission from the Senior Leadership team for exceptional access to the above areas for specific curriculum needs.

Students will be advised on security and never to give out personal details of any kind which may identify them or their location. Students will be advised to set strong passwords, to deny access to unknown individuals and to know how to block unwanted communications. This is aligned to the Schools Social Media Policy and designed to provide awareness to staff and safeguard our students from issues such as grooming or cyber-bullying.

Educational use of Videoconferencing and Webcams

The Purbeck School recognise that videoconferencing and the use of webcams can be a challenging activity but brings a wide range of learning benefits.

- All videoconferencing and webcam equipment will be switched off when not in use and will not be set to auto-answer.
- Videoconferencing contact details will not be posted publicly.
- Videoconferencing equipment will not be taken off the premises without prior permission from the DSL.
- Staff will ensure that external videoconferencing opportunities and/or tools are suitably risk assessed and will ensure that accounts and systems used to access these events are safe and secure.
- Video conferencing equipment and webcams will be kept securely and, if necessary, locked away or disabled when not in use.

Digital & Video images

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 preferably be taken on school equipment; the personal equipment of staff should ideally not be used for such purposes. They should also only be stored on the school network and not on any personal device. Care should be taken when taking digital/video images to ensure that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

Students should 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 and will comply with good practice guidance on the use of such images. All staff have a duty to educate students on the correct use of digital video and images.

Online public communications

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/pupils 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 a member of Senior Leadership Team, 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, VLE 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.

- All Students are provided with individual school email addresses for educational use. 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.

Section 13: Education

Children & Young People

The Internet is an essential element in 21st century life for education, business and social interaction. The Purbeck School is aware that there are e-safety issues that can put our students at risk such as 'sexting', online grooming and access to unsuitable material such as pornography. The school has a duty to provide students with a safe, high quality internet access as part of their learning experience. Internet use is a part of the statutory curriculum and a necessary tool for staff and students. A planned e-safety programme will be provided as part of ICT this will be overseen by the Head of Computing. Key e-safety messages will be reinforced as part of a planned programme of assemblies and activities within the PSHE programmes and tutor programmes.

Students will be taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information in order to be responsible users of the internet and stay safe.

Students should be helped to understand the need for the student AUP 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. Rules for use of ICT systems / internet will be posted in all ICT suites. Staff should act as good role models in their use of ICT, the internet and mobile devices.

Students will contribute to the development and review of E-Safety procedures. This will provide them with an opportunity to suggest improvements to current systems. Students will be encouraged to take part in e-safety activities, assemblies, lessons and parent sessions.

Internet use will enhance learning

- The Purbeck School Internet access will be designed expressly for student use and will include filtering appropriate to the age of students.
- Students will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- 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 how to evaluate Internet content

- Schools should ensure that the use of Internet derived materials by staff and by students complies with copyright law.

- Students should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

This aims to support and protect students by encouraging them to responsible if they are faced with e-safety issues such as phishing/copycat websites and warning them to use safe environments by educating them on pop-ups in the importance of protecting your personal information when using online facilities during both school and in their social time.

Professional standards

The Purbeck School provides professional development for staff on e-safety awareness; this is aimed to provide up to date information and inform staff of their wider professional responsibilities as set out in the Standards for Teachers part two. This highlights the responsibility of the teacher to safeguard students' well-being in accordance with statutory provision.

	E-safety training and education	**Communication methods**
Staff	In school programmes	VLE and school website Dorset E-Safety newsletter
Parents	Newsletters to be shared and message raised via parent mail. Information events	School website with links to other agencies provide current information Student work
Governors	Updates through School Development Group	School website Meetings Training
Students	Updates and news. Education about how to stay safe online and on appropriate use of the internet	PSHE ICT/ Computing lessons Tutor programme Assemblies School website

Parents/ Carers

Parents and carers may only have 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 / regulation of the children's on-line experiences. Parents can 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 should do about it.

The school will therefore seek to provide information and awareness to parents and carers through links and policies on the school web site and parent carer information events.

Section 14: Infrastructure

Passwords
Currently there is no agreed password policy however students will be advised to set strong passwords and encouraged to change them regularly. Posters for advice on setting a strong password will be on display in all networked rooms and also delivered in E-safety schemes of learning, PSHE and the tutor programme.

Connectivity and Filtering

Internet access is filtered for all users. Differentiated internet access is available for staff and customised filtering changes are managed by the school. Illegal content is filtered by broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and other illegal content lists. Filter content lists are regularly updated and internet use is logged and frequently monitored. The monitoring process alerts the school to breaches of the filtering policy, which are then acted upon. There is a clear route for reporting and managing changes to the filtering system. Where personal mobile devices are allowed internet access through the school network, filtering will be applied that is consistent with school practice.

The IT Manager carries out regular filtering reports on internet searches for both students and staff and any incidents reported are logged and sanctioned as per the school's behaviour policy.

Technical Security

The school will be responsible for ensuring that the school network is as safe and secure as is reasonably possible 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.

School ICT systems will be managed in ways that ensure that the school meets the e-safety technical requirements outlined in the SWGfL Security Policy and Acceptable Usage Policy and any relevant Local Authority E-Safety Policy and guidance. There will be regular reviews and audits of the safety and security of school ICT systems

Personal Data

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

The school will follow advice from the Local Authority or other relevant bodies regarding the management of data. Guidance regarding how long data will be kept is contained within an appendix to this policy and guidance.

Staff must ensure that they take care at all times to ensure the safe keeping of personal data and minimise the risk of its loss or misuse. The must 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, also where possible use encryption when transferring data.

Section 15: Standards & Inspection

Monitoring & reporting on e-safety incidents

The School will take all reasonable precautions to prevent access to inappropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Students have been made aware (Acceptable Use Agreement) that they must report any incident of unsuitable material.

Neither the school nor its staff can accept liability for the material accessed or any consequences of internet access. Where students are undertaking off-site educational activities, the risk assessment procedure will incorporate E-Safety issues.

Concerns about E-Safety, including cyber-bullying, will be dealt with initially by the DSL (or deputy DSL). An incident log will be maintained, including details of actions taken.

Complaints will be dealt with according to the Complaints Procedure Policy. Any complaint about staff misuse must be referred to the Headteacher.

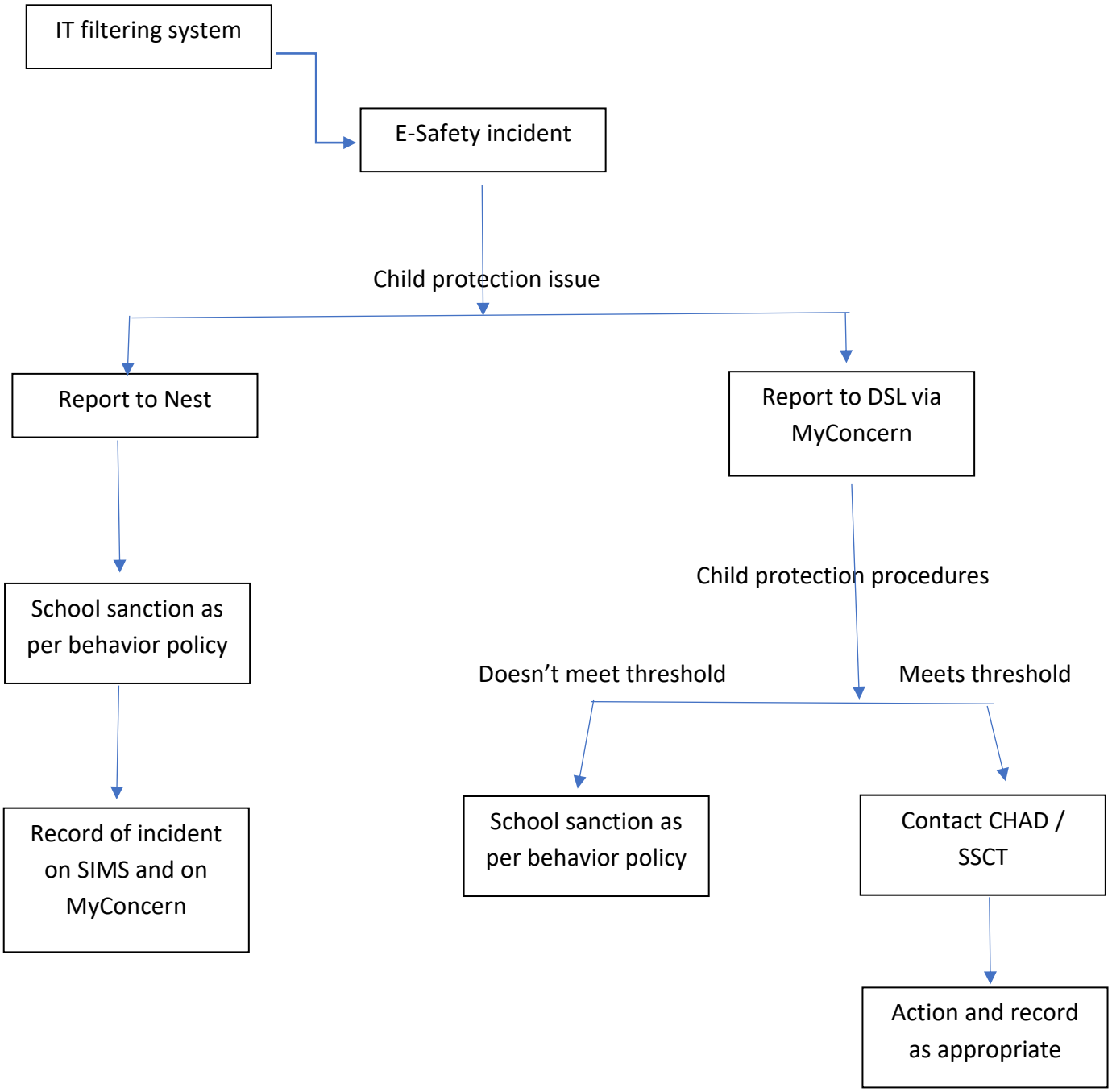
Incidents impacting Child Protection will be dealt with in accordance with the Child Protection Policy. Dorset Police advice will be sought on potentially illegal issues.

The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to Dorset Police.

Impact of the E-Safety Policy and Practice

The School will audit ICT use to establish if the E-Safety Policy is adequate and that the implementation of the E-Safety Policy is appropriate. Annual reviews will be carried out of E-safety incident logs, bullying logs, survey of staff, students and parents.

Appendix A


IT filtering system
E-Safety incident
Child protection issue
Report to Nest
Report to DSL via MyConcern
School sanction as per behavior policy
Child protection procedures
Doesn't meet threshold
Meets threshold
Record of incident on SIMS and on MyConcern
School sanction as per behavior policy
Contact CHAD / SSCT
Action and record as appropriate

Glossary of terms

ICT- Information Communication Technology

DSL – Designated Safeguarding Lead

SLT- Senior Leadership Team

CP- Child Protection

AUP- Acceptable Use Policy

LA- Local Authority

SwGFL- South West Grid for Learning

SDG- School Development Group

CEOP- Child Exploitation and Online Protection

KS- Key Stage

NSPCC- National Society for the Prevention of Cruelty to Children

PSHE- Personal, Social, Health and Economic Education

SOL- Scheme of Learning

CAIC- Child Abuse Image Content