The Polesworth School
ENSURING EXCELLENCE

Online Safety Policy

Member of leadership team with lead responsibility for oversight and update of policy	DOW
Approved at SLT	July 2024
Approved by the School Standards Committee (SSC)	July 2024
Policy review cycle	Biennially
Policy review date	July 2026

Contents

1. Introduction

2. Roles and Responsibilities

3. Recognition & response

4. Concern about student safety or adult behaviour

5. Allegations against people who work with children

6. The risks posed by new technologies

7. Our response to online safety risks to students

8. Cyber bullying

9. Systems and procedures

10. Related documents and timescales

11. Further guidance and support

12. Appendix A: Student Agreement

Introduction

1. At The Polesworth School we encourage student engagement with Information and Communication Technology (ICT) as we believe that it enables them to learn, communicate and explore the world in new ways many young people are now skilled in using computers, games consoles, mobile phones and tablet computers. However, with this new technology we also acknowledge that there are also new risks.

   We believe that everyone in our school community is responsible for the welfare and safety of children and it is therefore crucial that all stakeholders understand what these risks are and how we can all work together to enjoy these new technologies safely.

2. Online safety is essentially about creating a safe environment when using ICT. This includes the use of the internet and social networking sites. This document is intended to outline the school's approach to preventing safeguarding issues, including cyber bullying, as well as detailing how we respond to online safety issues when they emerge.

3. The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:

   - **content:** One of the key benefits of the web is that it is open to all but, unfortunately, this also means that for example, those with extreme political, racist, sexual or other prejudiced views are able to publicise those opinions. Therefore, young people could be exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-semitism, radicalisation and extremism. In the case of pornography and indecent images of children, there is no doubt that the internet plays host to a large amount of legal and illegal material. Curiosity about pornography is a normal part of sexual development but young people may be shocked by some of the material online and it is not known what the long-term effects of exposure to such images may be. Seeking out some aspects of pornography is a criminal offence and could result in a criminal conviction.
   - **contact:** being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other criminal purposes.' The threat of physical danger is perhaps the most worrying and extreme risk associated with the use of the internet and other technologies and is probably the risk most reported by the media. A criminal minority make use of the internet and related services to make contact with young people. The intention of these individuals is to establish and develop relationships with young people with the sole purpose of persuading them into relationships which can

then progress to sexual activity. Child sex offenders will often target specific individuals, posing as a young person with similar interests and hobbies in order to establish an online 'friendship'.

- **conduct:** personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying.
- **commerce** - risks such as online gambling, inappropriate advertising, phishing and or financial scams.

4. *"As in any other area of life, children and young people are vulnerable and may expose themselves to danger - knowingly or unknowingly - when using the internet and other digital technologies. Indeed, some young people may find themselves involved in activities which are inappropriate or possibly illegal."*[1]

5. Students are permitted to use their own mobile phone networks whilst on the school site during social times and when the teacher allows them to do so in lessons. This access means that some children, whilst in school, might sexually harass, bully, share indecent images and view and share pornography and other harmful content via their mobile phone and smart technology.

   Our aim is to address these potential issues by regularly providing clear guidelines and information to students, their parents and staff about how to keep young people safe and by dealing rapidly with any emerging concerns through a consistent approach, as outlined in this document; this will invariably involve close communication with parents and where necessary, liaison with Children's Services, the Police and other relevant agencies.

Roles and Responsibilities

6. As a school we see it as our responsibility to respond to online safety concerns, irrespective of whether they occur inside or outside of school. Breaches to our school network protocols will be dealt with rapidly by our system administrators in liaison, where appropriate, with the Designated Safeguard Lead (DSL) and/or other relevant pastoral leaders. However, where the school receives information of a safeguarding nature concerning online activity which has taken place outside school, the school is equally committed to engaging with the students concerned and their parents to resolve the situation. Where we feel there is an ongoing risk to a young person, Children's Services and occasionally the Police, may be contacted to provide further support.

7. It is the responsibility of all members of our school community, including teaching and non-teaching staff, governors, volunteers and students, to prevent and tackle online safety issues.

8. In line with the school's Child Protection Policy, all online safety concerns should be shared at the earliest opportunity with the DSL or Deputy DSL and in any case before the end of the school day. The DSL is responsible for ensuring that staff are aware of what constitutes an online safety concern that would be necessary to report.

9. The DSL will report regularly to the safeguarding governor on incidents of online safety concerns and the subsequent actions and outcomes within the school.

10. The Headteacher is responsible for ensuring that online safety concerns are monitored and that staff remain appropriately trained to respond to such concerns. It is also the responsibility of the Headteacher to ensure that preventative work is ongoing with students and that awareness raising among parents is ongoing.

Recognition and response

11. All members of our school community should be alert to the possibility that:

    - A child may already have been/be being abused and the images may have been distributed on the internet or by mobile telephone;
    - An adult or older child may be grooming a child for sexual abuse, including for involvement in making abusive images. This process can involve the child being shown abusive images;
    - An adult or older child may be viewing and downloading child sexual abuse images;
    - Children are capable of abusing their peers online.

Concern about student safety or adult behaviour

12. Any member of staff who has a concern about a safeguarding issue should complete a green 'Logging a concern about a child' form and inform the Designated Safeguarding Lead (DSL) or one of the Deputy DSLs as a matter of urgency and before the end of the school day. If the concern is about a member of staff, a yellow form should be completed and given to the Headteacher only. A concern should be shared even where there is no evidence to support it.

13. The DSL/Deputy DSL/Headteacher should follow the procedure set out in the school's Child Protection and Safeguarding Policy to assess whether a referral should be made to Children's Services or the Local Authority Designated Officer (LADO).

14. If a decision is made not to make a referral, the school will still keep a record of the concerns in the student's confidential file for reference should further concerns emerge at a later date.

15. Where specific children are identified as abused in the production of indecent images of children, a Section 47 Enquiry should be carried out by Children's Services and The Polesworth School will work closely with Children's Services to support the students throughout this time.

16. It is important to be aware that the child may not want to acknowledge his/her involvement in such behaviour or admit its abusive nature and may resist efforts to be offered protection. This should not be a deterrent and The Polesworth School will work closely with other agencies in order to continue to monitor and assess the nature and degree of any risk to the child.

17. Where there is concern about an adult, but there is no identifiable child, a referral will be made to the Police and to Children's Services, enabling them to initiate an investigation.

Allegations against people who work with children

18. All members of our school community should be aware of their responsibility to follow safeguarding procedures if they have a concern that adult staff members or volunteers may be accessing indecent images of children. Employees of the school are regularly made aware of the Whistleblowing Policy and the Headteacher must follow Warwickshire Safeguarding Children's Board interagency procedures in dealing with such allegations. The Local Authority Designated Officer (LADO) holds the responsibility for ensuring that allegations against members of staff are properly investigated. The Polesworth School follows LADO procedures in all cases where it is alleged that a person who works with children has:

    - behaved in a way that has harmed a child, or may have harmed a child;
    - possibly committed a criminal offence against or in relation to a child;
    - behaved toward a child or children in a way that indicates she or he is unsuitable to work with children.

19. In operating the LADO procedures, the school must consider whether the allegation can be properly investigated if the person concerned remains in work. Schools can seek advice about suspension and alternatives to suspension, but the final decision remains with the school. It would be very unusual for the school not to take the advice of the LADO and if it were to do so, the LADO may decide to take the issue to the education secretary.

20. It is important that individuals suspected of accessing, creating or downloading indecent images of children are not alerted prior to the police undertaking their investigations as they may destroy computer evidence at

work or home. This has implications for managing allegations against people who work with children and means individuals may not initially be fully informed of reasons for their suspension.

21. Research into investigations of adults accessing child abuse images has identified that professional staff accessing such images may have access to children both in their occupation and in their personal lives. In such cases, a section 47 strategy discussion (Children Act 1989) will consider the need to assess risk both in relation to the occupation and in relation to the risk to any child within the family of the individual concerned. The Headteacher and/or the DSL will be involved in this strategy meeting.

The risks posed by new technologies

22. As with many new or and emerging technologies, the internet has brought unfamiliar challenges, some of which create actual or potential dangers for children and young people.

23. New technologies have offered children and young people revolutionary advances in communication with their peers and with the world. However, they also afford an opportunity for misuse and abuse. The main risks are in relation to sexual exploitation and the use of technology to bully and record physical abuse.

24. Some of the most common risks to children and young people are as follows:

    <u>Children viewing adult pornography</u>

    Children & young people often access adult pornography. However, the persistent viewing of material which is degrading, violent or sadistic or beyond the realms of normal curiosity can affect how young people can think about intimacy, themselves and their values and attitudes towards relationships and sexual development. Adult pornography can also be used by adults or young people as part of a grooming process.

    <u>Children abused through using the Internet and mobile phones</u>

    New technologies such as social network sites, APPs and gaming sites are often used by those wanting to sexually exploit children and young people. These perpetrators often exploit young people who are vulnerable by grooming them.

    Children can be coerced to take part in sexual activity online by abusers who employ specific conversational techniques. The grooming process is no different from that used by abusers offline. However, the whole abusive episode takes place online without physical contact between the child and perpetrator. The most common place for targeting these children is in social networking sites and chat rooms. When discovered, children will often deny

any such activities, due to both the grooming process and the shame that many children feel when discovered doing something that have been told not to reveal and about which they feel deep humiliation and fear.

Young people creating and sending indecent images of themselves to others

Occasionally young people choose, or are coerced, into creating and sending indecent images of themselves to others. This can sometimes be vulnerable individuals who have been made to feel special and have been convinced that the other person involved loves them, is attracted to them. Often the other individual might promise to delete the images or to keep them secret. This can lead to considerable distress for the victim if the abuser then chooses to publicise the images. It can also result in blackmail if the victim says no to creating and sending further, more explicit images.

Children, who create, view or download sexually abusive images of other children

Although some children plan to and purposefully download these images, others may have been forced to do so by peer group pressure or they may have been introduced to these sites by predatory adults as part of grooming for sexual abuse.

Young people creating or placing images of other young people online

The use of the internet as a tool for bullying is also becoming increasingly common. For example, physical assaults can be carried out and placed online with the intention of humiliating, compromising or exploiting the young person who is the subject of the image.

Children groomed online for sexual abuse offline

It is an offence to groom a child. Sometimes children are befriended online by individuals with the sole purpose of gaining their trust. Often, they may lie about their age and background to appeal to the young person, building up their trust until a point when they can suggest that they meet. While this is rare, research shows that in the UK, five per cent of children have met up with someone they had only spoken to online, while 11 per cent of children said they have received a sexual message and 1 in 100 reported sending a sexual message. (Research compiled by the Office of National Statistics (ONS), the figures are for the year ending March 2020 and children and cover young people aged 10 to 15.). This means that across England and Wales an estimated 682,000 young people exchanged online messages during the year in question with someone they had never met and 212,000 met up in person with someone they had only spoken to online.

Children made the subject of child abuse images or pseudo-images

Children who are the subject of child abuse images may suffer incalculable trauma which may affect them for the rest of their lives. Perpetrators often use strategies to inhibit children disclosing the abuse: children may be shown abusive images of other children or their own abusive images in an attempt to normalise the activity; abusers may encourage children to place images of themselves or friends online; victims may be encouraged to be proactive in either their own sexual abuse or that of other children.

Pseudo images may be created of particular children by the technological manipulation of existing photographs, art or cartoons. These images often have the same impact on the victim as non-pseudo images.

Cybercrime

Cybercrime is criminal activity committed using computers and/or the internet. It is broadly categorised as either 'cyber-enabled' (crimes that can happen off-line but are enabled at scale and at speed on-line) or 'cyber dependent' (crimes that can be committed only by using a computer). Cyber-dependent crimes include;

- unauthorised access to computers (illegal 'hacking'), for example accessing a school's computer network to look for test paper answers or change grades awarded;
- denial of Service (Dos or DDoS) attacks or 'booting'. These are attempts to make a computer, network or website unavailable by overwhelming it with internet traffic from multiple sources; and,
- making, supplying or obtaining malware (malicious software) such as viruses, spyware, ransomware, botnets and Remote Access Trojans with the intent to commit further offence, including those above.

Children with particular skill and interest in computing and technology may inadvertently or deliberately stray into cyber-dependent crime.

Our response to online safety risks to students

25. In all cases of online safety concern, The Polesworth School follows the school's Child Protection and Safeguarding Policy to ensure concerns are reported appropriately as a matter of urgency and on the same day of a concern emerging, to the DSL or the DDSL. Where a risk is deemed to exist, parents, Children's Services and where appropriate, the Police will be informed. An assessment will usually be carried out by Children's Services to ensure that victims are fully protected and that the behaviour of child perpetrators is fully addressed.

26. Where it is felt that an ongoing risk is not a concern, the school is likely, usually following advice from Children's Services, to deal with the issues

directly with students and their parents. This may involve meetings with students and parents whereby boundaries/ restrictions to internet access may be imposed. The school may choose to involve external agencies as a way of educating young people further about risk, online safety. For child perpetrators, this may involve work which focuses on respecting themselves and others. Additionally, short courses run by our school counsellors may be used to educate, with the intention of altering perceptions and behaviour. These sessions address the school's moral and ethical stance, provide information for victims and their families and friends of where to go and what will happen next, as well as outlining the consequences for perpetrators.

27. Education is the key to minimising the online risks to students. Tutorial sessions, Assemblies and Enhanced Learning Sessions throughout the year are used regularly to educate students on appropriate online behaviour. These sessions address the following:

    - our approach to cyber bullying, with specific reference to our Anti Bullying Policy;
    - the safe use of social media, including utilising privacy settings and the pitfalls of sharing personal information and photographs;
    - the significance and consequences of their online behaviour, including digital footprints, legal sanctions and career prospects;
    - online stranger danger, including how to recognise and report suspicious activity;
    - the school's response to online behaviour that may bring the school or its members into disrepute.

28. The Child Exploitation and Online Protection Command (CEOP, http://www.ceop.police.uk/) brings together law enforcement officers and specialists from children's charities and industry to tackle online child sexual abuse. CEOP provides a dedicated 24 hour online facility for reporting instances of online child sexual abuse. CEOP's 'Report Abuse' button is on the home page of our school's website and every year students are informed of how to use this facility to report online abuse.

29. If there are concerns about a child in the area of cyber crime , the DSL (or a deputy), will consider referring into the **Cyber Choices** programme. This is a nationwide police programme supported by the Home Office and led by the National Crime Agency, working with regional and local policing. It aims to intervene where young people are at risk of committing, or being drawn into, low level cyber-dependent offences and divert them to a more positive use of their skills and interests. The **Cyber Choices** does not currently cover 'cyber-enabled' crime such as fraud, purchasing of illegal drugs on-line and child sexual abuse and exploit.

30. Annual training for all staff and new staff induction sessions, highlight the school's Social Networking Policy which informs all staff of our expectations in terms of protecting their identity and upholding an online presence that is appropriate to their professional position. All staff are made aware that it is a breach of our Social Networking Policy to have students as 'friends' on social media and that students and staff members should not communicate via personal telephone or email accounts. Staff are also made aware that their online posts which may bring the school into disrepute are not acceptable under the Social Networking Policy.

31. Mailings to parents and carers via the school newsletter address safety issues associated with social media and online communities. These articles outline the measures parents can take to educate and protect their children at home as well as informing them of the school's approach in terms of prevention and response to concerns.

32. Pupils with SEND have an increased vulnerability to risk online, especially those with language and communication needs, or social communication difficulties. All staff are made aware of vulnerable groups during Child Protection training and the Inclusion team monitor and work closely with vulnerable students and, where necessary, their parents to ensure that they are safe online.

Cyber-bullying

33. Bullying may be defined as deliberately hurtful behaviour, usually repeated over a period of time, where it is difficult for those bullied to defend themselves. It can take many forms but the main types are:

    - physical (e.g. hitting, kicking, theft)
    - verbal (e.g. racist or homophobic remarks, threats, name-calling)
    - emotional (e.g. isolating an individual from the activities and social acceptance of their peer group)

    "The damage inflicted by bullying (including cyberbullying via the internet) can frequently be underestimated. It can cause considerable distress to children, to the extent that it affects their health and development or, at the extreme, causes them significant harm (including self-harm). All settings in which children are provided with services or are living away from home should have in place rigorously enforced anti-bullying strategies." (Paragraph 11.57, Working Together 2010).

34. New technologies have offered children and young people innovative advances in communication with their peers and with the world. However, they also afford an opportunity for misuse and abuse. Bullying through technology (cyber-bullying) can be devastating for the victim and unlike in

the real world, the victim can be targeted at any time day or night, home or school.

35. Bullying can include emotional and/or physical harm to such a degree that it constitutes significant harm. _All staff at The Polesworth School are aware of the need to be alert to cyber bullying and in line with our Behaviour and Discipline Policy and Anti Bullying Policy, staff are expected to report all instances of bullying, including racist and homophobic bullying, to their Head of Year or a member of the pastoral team, who will address these issues as a matter of urgency.

36. More serious cases of bullying or ongoing bullying following intervention should be discussed with the school's DSL/DDSL and could involve making a referral to Children's Services. **Separate referrals for assessment and support may be made in respect of both child victim and child abuser.**

37. Where the bullying involves an allegation of crime (threats of assault, theft, harassment) a referral may be made to the police.

38. Information about good practice in anti-bullying strategies (real & virtual) for schools, can be accessed at;
https://**www.gov.uk**/.../the-use-**and-effectiveness-of-anti-bullying-strategies**-in-schools

Student Acceptable Use

39. Students are responsible for using the digital technology systems in accordance with the Student Acceptable Use Agreement. Students are educated to:

- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- Understand the importance of reporting abuse, misuse or access to inappropriate materials and how to do so;
- Know and understand policies on the use of mobile devices. They should also know and understand policies on the taking/use of images and on online-bullying;
- Understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.

Student Acceptable Network and Internet Use Policy Agreement

This agreement is signed by students. It is supported by our expectations of social media and online use by all students as set out in the Social Networking Policy.

Student Guidelines:

Students are expected to follow all guidelines stated below as well as those given verbally by staff and to demonstrate ethical behaviour in using the network facilities. Students are also expected to realise that the opportunity to use the network and The Polesworth School facilities go hand in hand with using computer hardware, software, and the Internet in a responsible manner. Any actions that might harm the computer equipment or software, or impair its effective use, or showing disregard for the proper procedures set up for network access will not be tolerated. Before use, all students will receive an overview of the aspects of security and ethics involved in using The Polesworth School network.

1. Students must not allow others to use their account name and/or their password. To do so is a violation of the Acceptable Use Policy.
2. Any action by a student that is determined by his/her classroom teacher or a system administrator to constitute an inappropriate use of the Internet at The Polesworth School or to improperly restrict or inhibit others from using and enjoying the Internet is a violation of the Acceptable Use Policy.
3. Transmission of material, information or software in violation of any school policy, local or British law is prohibited and is a breach of the Acceptable Use Policy.

Student Agreement

- I understand that the school will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password.
- I will immediately report any unpleasant or inappropriate material or messages that makes me feel uncomfortable when I see it online.
- I will not upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others.
- I will not try (unless I have permission) 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 access, copy, remove or alter any other user's files, without the owner's knowledge and permission.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person / organisation who sent the email.
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.
- Where work is protected by copyright, I will not try to download copies.

Violating the Acceptable Use Policy may result in:

- Removal of internet access privileges
- Complete removal of the computer access privilege
- Sanctions in line with the school's Behaviour Policy
- Legal action including criminal prosecution under appropriate British laws

In order to ensure smooth system operations, the System Administrator has the authority to monitor all accounts. Every effort will be made to maintain privacy and security in this process. The Polesworth School's internet monitoring process is carried out by the Warwickshire Education Services Department.

Systems and procedures

40. **Infrastructure** - Procedures are in place to protect the school and its students from a malicious cyber-attack. All computer equipment is protected by the security of the school. All external doors to buildings are locked. Visitors to the site are booked in. Servers, PBXf and network storage are kept in locked rooms with restricted access. Network communications equipment is kept in locked cabinets. The school network is protected behind the Warwickshire County Firewall to protect from external malicious attack.

    Access to Servers and Network is limited to a few school technical staff and county support engineers. Individual user ids are used and are protected with strong passwords.

    Any attempt internally at unauthorised access to servers is logged by the forensic software. All user data is backed up daily. Critical servers are backed up weekly.

The school uses VLANs to separate curriculum and administration networks, restricting activity and access as appropriate.

41. **Downloading software** – In order to prevent unauthorised users downloading software on school devices, laptops and desktop PCs are protected by user names and passwords. Students are automatically blocked from downloading software and virus guards are installed so that staff who download software can do so safely.

42. **Passwords and security** – Access to school networks and devices is controlled through careful password procedures, whereby students are taught about password strengths in their ICT lessons, before setting strong passwords of six characters which include upper and lower case letters as well as either a symbol or a number. Additionally, each user has a home folder on the server which cannot be accessed by other users. Students and staff also have access to their own designated shared areas which contain resources. Staff can also access students' home folders.

    School IT induction for staff ensures that they are briefed on the dangers of viruses and attachments. Emails are regularly sent out reminding staff of the need to be vigilant.

43. **External service providers** – The school is cautious in using external internet services and as such, for third party vendors, it is required that any internet access for students is only provided through the school's internet filter and forensic software.

44. **Guest access** – Procedures are in place to provide internet access to temporary staff such as trainee teachers, through temporary user IDs. Guest wifi allows access to the internet but not the local school network.

45. **Internet filtering** – The school uses 'Smoothwall', a Firewall software package, to filter internet content. This is run on a proxy in school. All internet traffic goes out through the school Smoothwall so is filtered and monitored.

    PC software provides a forensic logging ability and inappropriate use or attempt is logged. These logs are actively monitored and responded to by the safeguarding team.

    Students are limited by blocking lists which restrict content. However different levels of blocking can be applied to different year groups. This is done on a request basis, linked to curriculum needs.

    Students and staff who attempt to access a blocked site are informed by a Smoothwall screen message. Additionally, the Acceptable Use Agreement includes statements on logging and monitoring of school ICT equipment.

Should a member of staff require the temporary lifting of a website restriction they are required to inform the ICT helpline in school and the information is logged. The log contains the following details: the name of the member of staff, the date, the URL, the reason, the reversion date, the person making the change, the year groups or staff using the site.

46. **Monitoring digital platforms -** user logins, user printing, user door access, internet access and inappropriate activity on PCs and laptops are all monitored and reported to the appropriate school leader if concerns arise. The safeguarding team receive regular reports from the Digital Safeguarding Team at Warwickshire County Council and meet with students who have attempted to visit blocked sites, searched for inappropriate content or used language that prompts a safeguarding response.

47. **Staff training** ensures that staff are aware of the monitoring and filtering systems in place and reminds staff of their monitoring responsibilities when students are permitted to use their own mobile devices in lessons or when they use school owned devices. Staff must provide effective supervision, maintain awareness of how devices are being used by students and report any concerns to the Designated Safeguarding Lead.

48. **Reviews** occur annually and throughout the academic year as required. When concerns are identified they are escalated through the leadership team and the safeguarding team as appropriate.

Related documents and timescales

49. This policy should be read in conjunction with the following policies and procedures:

    - Child Protection and Safeguarding Policy
    - Behaviour and Discipline Policy
    - Social Networking Policy
    - Whistleblowing Policy
    - ICT Acceptable Use Policy
    - Child on Child Abuse Policy

50. The DfE's Filtering and Monitoring and Digital and Technology Standards have been consulted in the production of this policy and the Acceptable Use Policies. In addition to KCSIE, 2024, Teaching Online Safety in Schools, 2019, statutory RSHE guidance, 2019, and other relevant statutory and non-statutory guidance supports this policy.

51. This policy will be reviewed biennially following consultation with students, relevant staff and governors.

Further guidance and support

For professionals:

- Warwickshire Safeguarding Children Board; https://www.safeguardingwarwickshire.co.uk/

  On this inter-agency web-site there is specific web-site information and an 'online safety toolkit' designed to offer support and guidance.

- The UK Council for Child Internet Safety (UCCIS) https://www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis brings together over 160 stakeholders from across the internet safety spectrum who have come together to work in collaboration for the good of children and families.

- The Child Exploitation and Online Protection Centre (CEOP, www.ceop.police.uk/safety-centre/) brings together law enforcement officers, specialists from children's charities and industry to tackle online child sexual abuse. CEOP provides a dedicated 24-hour online facility for reporting instances of online child sexual abuse.

- https://www.thinkuknow.co.uk/ – a website for professionals (and children, young people and parents) full of information and resources about staying safe online.

- The Virtual Global Taskforce (VGT) https://nationalcrimeagency.gov.uk/virtual-global-taskforce/ was created in 2003 as a direct response to lessons learned from investigations into online child abuse around the world. It is an international alliance of law enforcement agencies working together to make the Internet a safer place.

- https://www.iwf.org.uk/ - This is an organisation, which works with the Police and Internet Service Providers to trace those responsible for putting harmful or illegal material on the web. It also encourages web surfers who find harmful or illegal material to report it.

- "Stop it Now!" Campaign https://www.stopitnow.org.uk/

- For information on the Byron report: https://webarchive.nationalarchives.gov.uk/ukgwa/20130401151715/http:/www.education.gov.uk/publications/eOrderingDownload/DCSF-00334-2008.pdf

- The Government commissioned Dr Tanya Byron to conduct an independent review to consider the risks to children from exposure to potentially harmful or inappropriate material via the internet and computer games. This report entitled, *'Safer Children in a Digital World'* was subsequently published in March 2008 and detailed recommendations to improve the safety of children through offering clear guidance and standards for all agencies who work

with children and young people. To read the full report or summary, or to obtain further information for children and young people on the findings of the report, please use the following hyperlink:
https://dera.ioe.ac.uk/6881/

For children, young people and their carers:

The following information gives advice to parents and children in terms of considering the dangers and managing risks, as well as information about computer software and supervised chat rooms etc.

- https://www.thinkuknow.co.uk/parents/ - a website for children, young people, parents and professionals full of information about staying safe online.

Appendix A

Acceptable Online and Social Networking Use

Student Agreement

- I understand that the school will monitor my use of the systems, devices and digital communications.

- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password.

- I will immediately report any unpleasant or inappropriate material or messages that makes me feel uncomfortable when I see it on-line.

- I will not upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others.

- I will not try (unless I have permission) 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 access, copy, remove or alter any other user's files, without the owner's knowledge and permission.

- I will immediately report any damage or faults involving equipment or software, however this may have happened.

- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person / organisation who sent the email.
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.

- Where work is protected by copyright, I will not try to download copies.

- I will always be polite when communicating with other students online.

- I will not use abusive or strong language towards others, which may be humiliating and hurtful. I will not use any communication device whether provided by the school or personally owned to bully or harass others.

- I will not post or distribute images or videos of others without their permission.

- I will not post or send inappropriate images or videos of myself or others to anyone.

- I will not post offensive or inappropriate comments about the school or members of staff.

- I will not try and contact staff using my personal account.

- I will be aware of "stranger danger", when communicating online.

Violating the Acceptable Use Policy may result in:

- Removal of internet access privileges
- Complete removal of the computer access privilege
- Sanctions in line with the school's Behaviour Policy
- Legal action including criminal prosecution under appropriate British laws

- In order to ensure smooth system operations, the System Administrator has the authority to monitor all accounts. Every effort will be made to protect privacy and security in this process.

Student Name

Student Signature