Initial Policy:	May 2019
Policy Updated:	
Next Review:	
Key Person:	

E-Safety Policy

Principles

- To ensure that all members of the school community are E-Safety conscious and understand how to protect themselves online.
- To support pupils in developing strategies to manage and respond to risk and be empowered to build resilience online.
- To safeguard and protect all members of Boorley Park Primary School community online.

Boorley Park Primary School seeks to protect children and young people against the messages of all violent extremism including, but not restricted to, those linked to extreme Islamist ideology, or too Far Right / Neo Nazi / White Supremacist ideology, Irish Nationalist and Loyalist paramilitary groups, and extremist Animal Rights movements (See the Preventing Extremism and Radicalisation policy).

Practice

An online safety (e-Safety) curriculum is established and embedded throughout the whole school, to raise awareness regarding the importance of safe and responsible internet use amongst pupils. Education about safe and responsible use precedes internet access.

Each half term a specific aspect of e-safety is identified and taught to pupils at an age-appropriate level. Online safety (e-Safety) is included in the PSHE and Computing programmes of study, covering both safe school and home use. Ongoing elements of understanding e-safety are included in the whole curriculum. Boorley Park Primary School ensures that differentiated and ability appropriate online safety (e-Safety) education is given, with input from specialist staff as appropriate (e.g. SENCO).

Annually all staff and Governors have E-Safety training on how to maintain safety on-line.

Annually parents are invited to an event on E-Safety on how to ensure they know and understand how to keep themselves and their children safe on-line.

Pupils will be supported in reading and understanding the E-Safety and Internet Use Agreement for Pupils and Parents (See Appendix 2) in a way which suits their age and ability.

Passwords

Boorley Park Staff / Governors:

- Will be provided with a username and password.
- The password should be a minimum of 8 characters long and must include letters and numbers.
- The password must not include proper names or any other personal information about the user that might be known by others.
- Passwords shall not be displayed on screen, and shall be securely hashed (use of one-way encryption).
- To ensure that other systems are not put at risk if one is compromised passwords should be different for systems used inside and outside of school.

From year 3, all pupils are provided with their own unique username and private passwords to access school systems. Pupils are responsible for keeping their password private.

Cyber-bullying

Boorley Park Primary School embraces the advantages of modern technology in terms of the educational benefits it brings, however the school is mindful of the potential for bullying to occur.

Central to the School's anti-bullying policy is the belief that 'all pupils have a right not to be bullied' and that 'bullying is always unacceptable'.

The School also recognises that it must 'take note of bullying perpetrated outside School which spills over into the School'. Under powers granted by the EIA (Education and Inspections) 2006, the Headteacher is able to police cyber-bullying or any bullying aspects carried out by pupils even at home.

Definition of cyber-bullying
Cyber-bullying is an aggressive, intentional act carried out by a group or individual using electronic forms of contact repeatedly over time against a victim who cannot easily defend himself/herself.

By cyber-bullying, we mean bullying by electronic media such as:

- Bullying by texts or messages or calls on mobile phones.
- The use of mobile phone cameras to cause distress, fear or humiliation.
- Posting threatening, abusive, defamatory or humiliating material on websites, to include blogs, personal websites, social networking sites.
- Using e-mail to message others.
- Hijacking/cloning e-mail accounts.
- Making threatening, abusive, defamatory or humiliating remarks in chat rooms, to include Facebook, Bebo, Youtube and Ratemyteacher and the like.

Legal issues
Cyber-bullying is not a specific offence but may in some instances be contrary to the civil or criminal law. In particular:

- It is unlawful to disseminate defamatory information in any media including internet sites.
- Section 127 of the Communications Act 2003 makes it an offence to send, by public means of a public electronic communications network, a message or other matter that is grossly offensive or one of an indecent, obscene or menacing character.
- The Protection from Harassment Act 1997 makes it an offence to knowingly pursue any course of conduct amounting to harassment.
- Section 1 of the Malicious Communications Act 1988 makes it an offence to send an electronic communication which is indecent or grossly offensive, or which conveys a threat, or which is false where there is an intention to cause distress or anxiety to the recipient.

Practice
The school educates its pupils both in the proper use of telecommunications and about the serious consequences of cyber-bullying and will, through Computing lessons, PSHE lessons and assemblies, continue to inform and educate its pupils in these fast changing areas.

The school trains its' staff to respond effectively to reports of cyber-bullying or harassment and has systems in place to respond to it.

The school endeavours to block access to inappropriate web sites, using firewalls, antivirus protection and filtering systems and no pupil is allowed to work on the internet in the Computer Room, or any other location within the school which may from time to time be used for such work, without a member of staff present.

Where appropriate and responsible, the school audits ICT communications and regularly reviews the security arrangements in place.

Whilst education and guidance remain at the heart of what we do, we reserve the right to take action against those who take part in cyber-bullying. All bullying is damaging but cyber-bullying and harassment can be invasive of privacy at all times. These acts may also be criminal acts.

- The school supports victims and, when necessary, will work with the Police to detect those involved in criminal acts.

- The school will use, as appropriate, the full range of sanctions to correct, punish or remove pupils who bully fellow pupils or harass staff in this way, either in or out of school.

- The school will use its power of confiscation where necessary to prevent pupils from committing crimes or misusing equipment.

- All members of the School community are aware they have a duty to bring to the attention of the Headteacher any example of cyber-bullying or harassment that they know about or suspect.

Responsibilities

The school leadership team will:

- Develop, own and promote the online safety vision and culture to all stakeholders, in line with national and local recommendations with appropriate support and consultation throughout the school community.
- Ensure that online safety is viewed by the whole community as a safeguarding issue and proactively developing a robust online safety culture.
- Support the Designated Safeguarding Lead (DSL) by ensuring they have sufficient time and resources to fulfil their online safety role and responsibilities.
- Ensure there are appropriate and up-to-date policies and procedures regarding online safety including the Staff ICT Code of Conduct (including the Acceptable Use Policy) which covers appropriate professional conduct and use of technology.
- Ensure that suitable and appropriate filtering and monitoring systems are in place to protect children from inappropriate content which meet the needs of the school community whilst ensuring children have access to required educational material.
- Work with and support technical staff in monitoring the safety and security of school/setting systems and networks and to ensure that the school/setting network system is actively monitored.
- Ensure all members of staff receive regular, up-to-date and appropriate training regarding online safety roles and responsibilities and provide guidance regarding safe appropriate communications.
- Be aware of any online safety incidents and ensure that external agencies and support are liaised with as appropriate.
- Ensure there are robust reporting channels for the school/setting community to access regarding online safety concerns, including internal, local and national support.
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology, including ensuring the safe and responsible use of devices.

All staff members will:

- Contribute to the development of online safety policies.
- Read the school ICT Staff Code of Conduct (including the Acceptable Use Policy (AUP)), and adhering to them.
- Have an awareness of a range of different online safety issues and how they may relate to the children in their care.
- Model good practice when using new and emerging technologies
- Embed online safety education in curriculum delivery wherever possible.
- Identify individuals of concern and take appropriate action by following school safeguarding policies and procedures. Know when and how to escalate online safety issues, internally and externally.
- Maintain a professional level of conduct in their personal use of technology, both on and off site.

Staff managing the school network (through the Wildern Academy trust) will:

- Provide a safe and secure technical infrastructure which support safe online practices while ensuring that learning opportunities are still maximised.
- Take responsibility for the implementation of safe security of systems and data in partnership with the leadership and management team.
- Ensure that suitable access controls and encryption is implemented to protect personal and sensitive information held on school-owned devices.

- Ensure that the school's filtering policy is applied and updated on a regular basis and that responsibility for its implementation is shared with the DSL.
- Ensure that the use of the school/setting's network is regularly monitored. Report any breaches or concerns to the DSL and leadership team and together ensure that they are recorded and appropriate action is taken as advised.
- Ensure that the school's ICT infrastructure/system is secure and not open to misuse or malicious attack.
- Ensure that appropriate anti-virus software and system updates are installed and maintained on all setting machines and portable devices.

The E-Safety Coordinator:

- Leads the E-Safety pupil focus group.
- Takes day-to-day responsibility for E-Safety issues and has a leading role in establishing and reviewing the school E-Safety policies / documents.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an E-Safety incident taking place.
- Provides training and advice for staff.
- Liaises with the Local Authority / relevant body when applicable.
- Liaises with school technical staff.
- Receives reports of E-Safety incidents and creates a log of incidents to inform future E-Safety developments.
- Meets regularly with E-Safety Governor to discuss current issues.
- Reports regularly to Senior Leadership Team.

The 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 monitoring the E-Safety policy including the impact of initiatives.

Members of the E-Safety Group will assist the E-Safety Coordinator with:

- The production / review / monitoring of the school E-Safety policy / documents.
- Mapping and reviewing the E-Safety curricular provision – ensuring relevance, breadth and progression.
- Monitoring network / internet / incident logs.
- Consulting stakeholders – including parents / carers and the pupils about the E-Safety provision.

Responding to Online Incidents and Safeguarding Concerns

- All members of the school/setting community will be informed about the procedure for reporting online safety (e-Safety) concerns, such as breaches of filtering, sexting, cyberbullying, illegal content etc.
- The Designated Safeguarding Lead (DSL) will be informed of any online safety (e-Safety) incidents involving child protection concerns, which will then be recorded. The DSL will ensure that online safety concerns are escalated and reported to relevant agencies in line with the Hampshire Safeguarding Children Board (SSCB) thresholds and procedures.
- Complaints about Internet misuse will be dealt with under the School's complaints procedure.
- Complaints about online bullying will be dealt with under the School's anti-bullying policy.
- Any complaint about staff misuse will be referred to the headteacher. Any allegations against a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer).
- All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community.

- The school will manage online safety (e-Safety) incidents in accordance with the school behaviour policy where appropriate. The school will inform parents/carers of any incidents of concerns as and when required.
- Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the Education Safeguarding Team or Hampshire Police via 101 or 999 if there is immediate danger or risk of harm.

Linked Policies : Anti-Bullying Policy
Behaviour Policy
British Value Statement
Child Protection Policy
Complaints Policy
Code of Conduct
Data Protection Policy
Information Communication Technology (ICT) Policy
Preventing Extremism and Radicalisation
Safeguarding Policy
Whistleblowing (Protected Disclosures) Policy

Appendix 1: Guidance on Cyber bullying

a) Staff

If you suspect or are told about a cyber-bullying incident, follow the protocol outlined below:

Mobile Phones

- Ask the pupil to show you the mobile phone.
- Note clearly everything on the screen relating to an inappropriate text message or image, to include the date, time and names.
- Make a transcript of a spoken message, again record date, times and names.
- Tell the pupil to save the message/image.
- Inform a member of the Senior Leadership team and pass them the information that you have.

Computers

- Ask the pupil to get up on-screen the material in question.
- Ask the pupil to save the material.
- Print off the offending material straight away.
- Make sure you have got all pages in the right order and that there are no omissions.
- Inform a member of the Senior Leadership team and pass them the information that you have.
- Normal procedures to interview pupils and to take statements will then be followed particularly if a child protection issue is presented.

b) Pupils

If you believe you or someone else is the victim of cyber-bullying, you must speak to an adult as soon as possible. This person could be a parent/guardian, or a member of staff at Boorley Park Primary School.

- Do not answer abusive messages but save them and report them.
- Do not delete anything until it has been shown to your parents/guardian or a member of staff at Boorley Park Primary School (even if it is upsetting, the material is important evidence which may need to be used later as proof of cyber-bullying).
- Do not give out personal IT details.
- Never reply to abusive e-mails.
- Never reply to someone you do not know.
- Stay in public areas in chat rooms.

c) Parents

It is vital that parents and the school work together to ensure that all pupils are aware of the serious consequences of getting involved in anything that might be seen to be cyber-bullying. Boorley Park Primary School informs parents of the cyber-bullying policy and the procedures in place to deal with cyber-bullying.

- Parents can help by making sure their child understands the school's policy and, above all, how seriously Boorley Park Primary School takes incidents of cyber-bullying.
- If parents believe their child is the victim of cyber-bullying, they should save the offending material (if need be by saving an offensive text on their or their child's mobile phone) and make sure they have all relevant information before deleting anything.
- Parents should contact the school as soon as possible. A meeting can then be arranged with a member of the Senior Leadership Team.

E-Safety at home

Several sites offer helpful advice to parents, particularly with respect to how they can best monitor their child's use of the computer at home. Important and useful information and links can be found on the school website.

Appendix 2
E-Safety and Internet Use Agreement for Parents and Pupils

Parents are encouraged to:

- Discuss online safety issues with their children, supporting the school in their online safety approaches, and reinforcing appropriate safe online behaviours at home.
- Role model safe and appropriate uses of technology and social media.
- Identify changes in behaviour that could indicate that their child is at risk of harm online.
- Seek help and support from the school, or other appropriate agencies, if they or their child encounters online problems or concerns.

Pupils are encouraged to:

- Develop their ICT skills and general research skills.
- Engage in online learning activities including games and quizzes
- Develop and apply their e-safety awareness and understanding of the “SMART Rules”.

Pupils are not permitted to:

- Download software or other files without permission (of parents and teachers).
- Send inappropriate messages or engage in inappropriate, abusive or defamatory chat and forums.
- Publish, share or distribute personal information about any user (such as home address, email address, phone numbers, photos etc).
- Use another person’s login and password or allow other users to use their login and password.

Sanctions:

- Verbal warnings – These are given for attempts to contravene the rules. This will be followed by a written letter to parents stating what has occurred. The pupils internet use at school will then be monitored for a 4 week period.
- In some cases, the child will lose access rights to the school internet for an appropriate period of time. This decision will be made by the Headteacher.

Appendix 3
Pupil E-safety Agreement (Reception)

These rules will help to keep everyone safe and help us to be fair to others.

- I will only go on apps that adults have told me to go on
- I will only visit internet sites that are appropriate for my age.
- I will only talk online with people I have met and know.
- I will only send kind messages.
- I will not open anything unless I have been given permission by an adult.
- I will not post anything online without telling an adult.
- If I see anything I do not like, I will show an adult.

My name: . . . . . .
My class: . . . . . .

Parent E-safety Agreement

As the parent or legal guardian, I have read and understood the attached school e-safety rules and grant permission for my daughter or son to have access to use the internet and other ICT facilities at school.

We have discussed the e-safety rules attached to this document and my daughter or son agrees to follow the rules and to support the safe and responsible use of ICT at Boorley Park Primary School.

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the internet and devices, but I understand that the school will take every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. These steps include using an educationally filtered service, restricted access, employing appropriate teaching practice and teaching e-safety skills to pupils.

I understand that the school can check my child's computer files and the internet sites that they visit, and that if they have concerns about their e-safety or e-behaviour they will contact me.

I understand the school is not liable for any damages arising from my child's use of the internet facilities.

I will support the school by promoting safe use of the internet and digital technology at home and will inform the school if I have any concerns over my child's e-safety.

Child's name: ……..
Child's class: ……..
Parent/Guardian signature: ……..
Date ……

Appendix 4
Pupil E-safety Agreement (KS1 and KS2)

These rules will help to keep everyone safe and help us to be fair to others.

- I will only use the school's computers for schoolwork and homework. When in a club, I will make sure to use them appropriately and go on the programs that the adults have told me to.
- I will not tell anyone my login and password.
- I will only login to the school systems as myself.
- I will only edit or delete my own files once I have asked an adult.
- I am aware that some websites and social networks have age restrictions which mean that I should not go on them.
- I will only visit internet sites that are appropriate for my age.
- I will only communicate with people I know, or that a responsible adult has approved.
- I will only send polite and friendly messages.
- I will not open an attachment, or download a file, unless I have been given permission by an adult.
- I will not tell anyone my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless a trusted adult has given permission.
- If I see anything I am unhappy with or I receive a message I do not like, I will show a responsible adult.

My name: . . . . . .
My class: . . . . . .
Date: . . . . . .