PHOENIX PLACE

Online Safety Policy

Independent School Standards:
paragraphs 7 and 34.

This policy pays regard to the latest 'Keeping Children Safe in Education' (September, 2024) statutory safeguarding guidance, and the DfE's 'Teaching online safety in schools' guidance (June, 2019).

Updated:	September 2024
To be reviewed:	August 2025
Reviewed and approved by Proprietor/Director:	Sophie Nelson
Reviewed and approved by (Strategic Advisory Partners)	*Currently recruiting*
Relationship to other school policies	**This policy should be read in conjunction with** ★ Child protection / safeguarding policy ★ Behaviour policy ★ Staff disciplinary procedures / code of conduct ★ Data protection policy and privacy notices ★ Complaints procedure ★ ICT and internet acceptable use policy
Reviewed	Annually

Introduction **3**

Aims: The aims of this Online/E-safety Policy is to: 4

Legislation and guidance 4

Monitoring and Review 4

Roles and responsibilities 5

The headteacher: 5

The Strategic Advisory Partner (SAP - 'governance) 5

The Designated Safeguarding Lead (DSL): 5

The ICT manager 6

All staff and volunteers 6

Pupils 7

Parents and Carers 7

Visitors and members of the community 7

Educating pupils about online safety 7

Using the Internet 7

The Curriculum 8

Educating parents about online safety 9

Cyber-bullying 9

Definition 9

Preventing and addressing cyber-bullying 9

Examining electronic devices 9

Artificial intelligence (AI) 10

Acceptable use of the internet in school 11

Staff using work devices outside school 11

How the school will respond to issues of misuse 11

Training 11

Monitoring arrangements 12

Appendix 1: KS3 and KS4 acceptable use agreement (pupils and parents/carers) 13

Appendix 2: Acceptable use agreement (Students, Parents/carers) 15

Appendix 3: Acceptable use agreement (staff, 'governors', volunteers and visitors) 16

Appendix 4: online safety training needs – self-audit for staff 17

Appendix 5: TIPS: CYBER BULLYING -WHAT CAN YOU DO ABOUT IT? 18

Appendix 6: Glossary of cyber security terminology 20

Introduction

PhoenixPlace recognises that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all pupils and staff are protected from potential online harm. This policy has been written with the particular needs of PhoenixPlace's pupils in mind.

Staff are aware that students with learning difficulties are vulnerable and may expose themselves to greater risks online and that children with special educational needs are more likely to be persistently cyberbullied over a prolonged period of time. Therefore, we recognise that our pupils may require additional teaching, including reminders, prompts and further explanations to reinforce their existing knowledge and understanding of ICT issues and appropriate and safe online behaviour. It is crucial that we explicitly teach our pupils that online actions can have offline consequences.

The Headteacher and School Leadership Team have taken the decision that, due to the nature of our pupils' difficulties and with the objective of keeping everyone safe, pupils are not allowed access to their personal mobile phones/devices during the school day.

Children, young people and adults interact with technologies such as mobile phones, games consoles and the internet on a daily basis and experience a wide range of opportunities, attitudes and situations. The exchange of ideas, social interaction and learning opportunities involved are greatly beneficial to all, but can occasionally place children, young people and adults at risk.

The school identifies that the internet and associated devices are an important part of everyday life which present positive and exciting opportunities, as well as challenges and risks and the Headteacher is aware of the school's responsibility to safeguard its pupils online as well as offline.

PhoenixPlace aims to empower and educate its pupils so that they are equipped with the skills to make safe and responsible decisions when using the internet and technology. Pupils will be taught to use the internet in a considered and respectful way and will develop their resilience so that they can manage and respond to online risks.

All members of staff understand that for young people there is no separation between 'real life' and the 'online world' and that technology is a significant component in many safeguarding and wellbeing issues.

- ★ Staff are aware that children and young people are at risk of abuse online as well as face to face and, in many cases, abuse will take place concurrently, sometimes involving each other.
- ★ All members of staff are aware of the importance of good e-safety practice in the classroom in order to educate and protect the pupils in their care.
- ★ Members of staff also need to be informed about how to manage their own professional reputation online and demonstrate appropriate online behaviours compatible with their role. The school has a Social Media Policy and Code of Conduct for staff to refer to.

The E-safety Policy is essential in setting out how the school plans to develop and establish its e-safety approach and to identify core principles which all members of the school community need to be aware of and understand.

Aims: The aims of this Online/E-safety Policy is to:

- ★ Safeguard and protect all members of the PhoenixPlace community online.
- ★ Identify approaches to educate and raise awareness of online safety throughout the community.
- ★ Enable all staff to work safely and responsibly, to role model positive behaviour online and to manage professional standards and practice when using technology.
- ★ Identify and support groups of pupils that are potentially at greater risk of harm online than others
- ★ Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- ★ Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

PhoenixPlace identifies that the issues classified within online safety are considerable but can be broadly categorised into four areas of risk:

- ★ **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- ★ **Contact** – being subjected to harmful online interaction with other users, such as 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 purposes
- ★ **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as 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; and
- ★ **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

Legislation and guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- ★ Teaching online safety in schools
- ★ Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- ★ Relationships and sex education
- ★ Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

Monitoring and Review

- ★ As technology evolves and changes rapidly, PhoenixPlace will review this policy annually, but will revise it following any national or local policy requirements, any child protection concerns or any changes to the technical infrastructure.
- ★ The school will regularly monitor internet use and evaluate online safety mechanisms to ensure that this policy is constantly applied.
- ★ The Headteacher is the e-safety coordinator and will be informed of any online safety concerns to ensure oversight of online safety.
- ★ Any issues identified will be incorporated into the school's action planning.

Teaching pupils about the safe use of technology is embedded throughout the curriculum (predominantly within our computing and PSHE education) and pupils are taught about online safety and risks as part of our whole-school approach.

This policy also pays regard to the government guidance issued by the UK Council for Internet Safety https://www.gov.uk/government/organisations/uk-council-for-internet-safety and should be read in conjunction with our 'keeping our pupils safe', 'personal development' and 'anti-bullying' policies, including staff discipline, conduct, capability & grievance procedures.

Roles and responsibilities

The Headteacher:

- ★ The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

The Strategic Advisory Partner (SAP - 'governance)

- ★ The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.
- ★ The governing board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.
- ★ The governing board will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.
- ★ The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).
- ★ The governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online.
- ★ The governing board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting the standards, which include:
    - Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
    - Reviewing filtering and monitoring provisions at least annually;
    - Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
    - Having effective monitoring strategies in place that meet their safeguarding needs.

The Designated Safeguarding Lead (DSL):

Details of the school's DSL and deputies are set out in our child protection / Safeguarding policy as well as relevant job descriptions.

The DSL and deputy DSL takes lead responsibility for online safety in school, in particular:

- ★ Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- ★ Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents

- ★ Managing all online safety issues and incidents in line with the school child protection policy
- ★ Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- ★ Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- ★ Updating and delivering staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs)
- ★ Liaising with other agencies and/or external services if necessary
- ★ Providing regular reports on online safety in school to the headteacher and/or governing board

This list is not intended to be exhaustive.

The ICT manager

The ICT manager is responsible for:

- ★ Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- ★ Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- ★ Conducting a full security check and monitoring the school's ICT systems on a monthly basis
- ★ Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- ★ Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- ★ Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- ★ Maintaining an understanding of this policy
- ★ Implementing this policy consistently
- ★ Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- ★ Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by emailing the ICT Manager regarding any failures and copying the DSL.
- ★ Working with the DSL to ensure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- ★ Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- ★ Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

Pupils

It is the responsibility of pupils (at a level that is appropriate to their individual age and ability) to:

- ★ Engage in age appropriate online safety education opportunities.
- ★ Read and adhere to the school's AUP for pupils.
- ★ Respect the rights and feelings of others both on and offline.
- ★ Take responsibility for keeping themselves and others safe online
- ★ Seek help from a trusted adult if there is a concern online and support others that may be experiencing online safety issues.

Parents and Carers

It is the responsibility of parents and carers to:

- ★ Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- ★ Read and sign the school's AUP for parents/carers and encourage their children to adhere to them.
- ★ Support the school's online safety approaches by discussing online safety issues with their children and reinforcing appropriate and safe online behaviours at home. The school will promote this through either emails or school newsletter
- ★ Role model safe and appropriate use of technology and social media.
- ★ Seek help and support from the school or other agencies, if they or their child encounter online issues.
- ★ Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies used by their children.

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- ➔ What are the issues? – UK Safer Internet Centre
- ➔ Hot topics – Childnet International
- ➔ Parent resource sheet – Childnet International
- ➔ Healthy relationships – Disrespect Nobody

Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3).

Educating pupils about online safety

Using the Internet

We have a duty to provide pupils with quality internet access as part of their learning experience. Pupils will be taught what internet use is acceptable and what is not and given clear objectives for its use. All staff involved with teaching and learning will prepare pupils to benefit safely from the opportunities presented and ensure that they have a growing understanding of how to manage the risks involved in online activity in the following ways.

- ★ Discussing, reminding or raising relevant online safety messages with pupils routinely, wherever suitable opportunities arise
- ★ Reminding pupils, colleagues and parents/carers about their responsibilities, which have been agreed through the User Agreement (Appendix 1) that all pupils and parents/carers have signed
- ★ Staff will guide pupils to online activities that will support the learning outcomes planned for the pupils' age and maturity. Access levels will also be reviewed to reflect curriculum requirements

- ★ Teaching pupils as a planned element of personal, social, health, economic and citizenship and computing education about online safety, cyber-bullying, misuse of technology, the law in this area and how to correctly use modern technology for positive reasons.

The Curriculum

Pupils will be taught about online safety as part of the curriculum:

It is also taken from the guidance on relationships education, relationships and sex education (RSE) and health education.

All schools have to teach:

- ★ Relationships and sex education and health education in secondary schools
- ★ The safe use of social media and the internet will also be covered in other subjects where relevant.
- ★ Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

Secondary schools

In **Key Stage 3**, pupils will be taught to:

- ★ Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- ★ Recognise inappropriate content, contact and conduct, and know how to report concerns

Pupils in **Key Stage 4** will be taught:

- ★ To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- ★ How to report a range of concerns

By the **end of secondary school**, pupils will know:

- ★ Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- ★ About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- ★ Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- ★ What to do and where to get support to report material or manage issues online
- ★ The impact of viewing harmful content
- ★ That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners
- ★ That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail
- ★ How information and data is generated, collected, shared and used online
- ★ How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
- ★ How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

Educating parents about online safety

The school will raise parents' awareness of internet safety in letters, on weekly reports or other communications home, and in information via our website. This policy will also be shared with parents.

The school will let parents/carers know:

- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL/ deputy DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

Cyber-bullying

Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. There will be an open dialogue by all staff to discuss cyber-bullying, and teaching staff are encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, trustees and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been shared among pupils, the school will use all reasonable endeavours to ensure the incident is contained and will work with outside agencies to support this and the young people affected.

The DSL will also consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

See appendix 5 for tips on dealing with Cyber-Bullying.

Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or

- ★ Is identified in the school rules as a banned item for which a search can be carried out, and/or
- ★ Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- ★ Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the headteacher / Pastoral Manager / DSL
- ★ Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- ★ Seek the pupil's co-operation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- ★ Cause harm, and/or
- ★ Undermine the safe environment of the school or disrupt teaching, and/or
- ★ Commit an offence

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL / headteacher or Deputy Head / Pastoral Manager to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- ★ They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- ★ The pupil and/or the parent/carer refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- ★ **Not** view the image
- ★ Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:

- ★ The DfE's latest guidance on searching, screening and confiscation
- ★ UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

PhoenixPlace recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

PhoenixPlace will treat any use of AI to bully pupils in line with our anti-bullyingManagement of Behaviour policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the school

Acceptable use of the internet in school

All pupils, parents/carers, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 to 3). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.

More information is set out in the acceptable use agreements in appendices 1 to 3.

Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- ★ Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- ★ Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- ★ Making sure the device locks if left inactive for a period of time
- ★ Not sharing the device among family or friends
- ★ Installing anti-virus and anti-spyware software
- ★ Keeping operating systems up to date – always install the latest updates

Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 3.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the ICT Manager/ Headteacher or School Business Manager.

How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour and appropriate use of ICT including mobile and smart technology. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- ★ Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- ★ Children can abuse their peers online through:
    - ○ Abusive, harassing, and misogynistic messages
    - ○ Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    - ○ Sharing of abusive images and pornography, to those who don't want to receive such content
    - ○ Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- ★ Develop better awareness to assist in spotting the signs and symptoms of online abuse
- ★ Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh the risks up
- ★ Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.
SAP members will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. Staff can log any issues/concerns via CPOMs.

This policy will be reviewed every year by the DSL, who is the online champion.

At every review, the policy will be shared with SAP members. The review will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

Appendix 1: KS3 and KS4 acceptable use agreement (pupils and parents/carers)

PHOENIXPLACE INTERNET E-SAFETY USE AGREEMENT

This describes the rules your child must follow when using the Internet throughout their School years. Both parents/carers and students must read this agreement to acknowledge the importance of your rights and responsibilities as users of the Internet in the School.

Students and parents then need to sign and return the ICT Use Agreement, this will be completed before the student starts.

- This agreement requires that students use the Internet and School network in a proper and responsible way, that you respect other users, and their rights and religions, and that you do not abuse School rules.
- The use of the Internet and Home-School access must be for education and for normal School work.
- Transmission of any material in violation of any UK laws is prohibited. This includes, but is not limited to copyrighted material, threatening or obscene materials and virus infected documents.
- The use of the Internet is a privilege, not a right, and inappropriate activity will result in you not being allowed to use School computers.
- A log of all computer activity and Internet access is monitored so misuse of the system by individuals can be quickly identified and dealt with.

Network Rules - You are expected to abide by the following rules:

A. Be polite. Never be abusive, or inappropriate, in your messages to others.
B. Illegal activities are strictly forbidden.
C. The use of external private or personal websites, social networking sites, chatrooms and messaging services are not permitted unless they are provided to all students by the School for a specific educational purpose under the direction of the teacher.
D. Do not reveal the personal address or phone number of students or colleagues to anyone.
E. Note that electronic mail (e-mail) is not private. The School will have access to all mail. Messages relating to, or in support of, illegal activities may be reported to the police. Only use the email system provided by the School.
F. Do not use the network in such a way that you would disrupt the use of the network by other users.
G. All communications and information accessible via the network should be assumed to be property of the School.
H. For certain Internet forums, discussion groups, user groups, servers, etc, which contain or address material that is, or could be construed to be obscene students and staff are expressly denied access to such Internet resources.
I. iEmail, files transfers, or file access is denied to these sites. Such addresses may not be book- marked, hot-listed, or otherwise included in individual student directories.
J. Students may not use another individual's account or login name and password.
K. Students may not access resources for which they do not have expressed permission. If you feel you can identify an access security problem on the School network, or Internet, you must notify a member of staff. Do not demonstrate the problem to other users.
L. Attempts to log-on to the Internet as a system administrator are specifically denied. Any such attempts will result in cancellation of users' privileges. Any user identified as a security risk may be denied access to the Internet and School computer resources.
M. Vandalism will result in cancellation of privileges. Vandalism is defined as any malicious attempt to harm or destroy any hardware or data of another user or any of the agencies or other networks that are connected to the Internet. This includes, but is not limited to, the uploading or creation of computer viruses.
N. Students who cause damage will be required to meet the cost of repair or replacement.
O. The School makes no warranties of any kind, whether expressed or implied, for the service it is providing.
P. The School will not be responsible for any damages, including the loss of data resulting from delays, non- deliveries, mis-deliveries, or service interruptions caused by its own negligence or your errors or omissions.
Q. The School specifically denies any responsibility for the accuracy or quality of information obtained through its services.

Appendix 2: Acceptable use agreement (Students, Parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Name of pupil:	**Year Group:**
I will read and follow the rules in the acceptable use agreement policy. **When I use the school's ICT systems (like computers) and get onto the internet in school I will:** · Always use the school's ICT systems and the internet responsibly and for educational purposes only · Only use them when a teacher is present, or with a teacher's permission · Keep my usernames and passwords safe and not share these with others · Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer · Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others · Always log off or shut down a computer when I've finished working on it **I will not:** · Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity · Open any attachments in emails, or follow any links in emails, without first checking with a teacher · Use any inappropriate language when communicating online, including in emails · Create, link to or post any material that is pornographic, offensive, obscene or otherwise inappropriate · Log in to the school's network using someone else's details · Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision **If I bring a personal mobile phone or other personal electronic device into school:** · I will not use it during lessons, tutor group time, clubs or other activities organised by the school, without a teacher's permission · I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online **I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.**	
Signed (pupil):	**Date:**
Parent/carer's agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 3: Acceptable use agreement (staff, 'governors', volunteers and visitors)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS	
Name of staff member/governor/volunteer/visitor:	
When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not: ● Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) ● Use them in any way which could harm the school's reputation ● Access social networking sites or chat rooms ● Use any improper language when communicating online, including in emails or other messaging services ● Install any unauthorised software, or connect unauthorised hardware or devices to the school's network ● Share my password with others or log in to the school's network using someone else's details ● Take photographs of pupils without checking with teachers first ● Share confidential information about the school, its pupils or staff, or other members of the community ● Access, modify or share data I'm not authorised to access, modify or share ● Promote private businesses, unless that business is directly related to the school	
I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 4: online safety training needs – self-audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	**Date**:
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

Appendix 5: TIPS: CYBER BULLYING -WHAT CAN YOU DO ABOUT IT?

Below are some tips to beat cyber bullying. In the first instance, students should inform an appropriate adult. This can be a parent/carer or staff at PHOENIXPLACE.

- If you're being bullied by phone or the Internet remember, bullying is never your fault. It can be stopped and it can usually be traced. Don't ignore the bullying. Tell someone you trust, such as a teacher or parent/carer, or call an advice line.
- Try to keep calm. If you are frightened, try to show it as little as possible. Don't get angry, it will only make the person bullying you more likely to continue. There's plenty of online advice on how to react to cyber bullying. For example, www.kidscape.org and www.wiredsafety.org have some useful tips.

Web Bullying

- If you don't know the owner of the website, refer to staff to find out how to get more information about the owner.

Chat rooms and instant messaging

- Never give out your name, address, phone number, School name or password online. It's a good idea to use a nickname. And don't give out photos of yourself.
- Don't accept emails or open files from people you don't know. Remember it might not just be people your own age in a chat room.
- Stick to public areas in chat rooms and get out if you feel uncomfortable.
- Tell your parents or carers if you feel uncomfortable or worried about anything that happens in a chat room.

Text/video messaging

- You can easily stop receiving text messages for a while by turning off incoming messages for a couple of days. This might stop the person texting you by making them believe you've changed your phone number. To find out how to do this, visit www.wiredsafety.org.
- If the bullying persists, you can change your phone number. Ask your mobile service provider (such as Orange, O2, Vodafone or T-Mobile).
- Don't reply to abusive or worrying text or video messages. Your mobile service provider will have a number for you to ring or text to report phone bullying. Visit their website for details.
- Don't delete messages from cyber bullies. You don't have to read them, but you should keep them as evidence.

Emails

- Never reply to unpleasant or unwanted emails — the sender wants a response, so don't give them that satisfaction.
- Keep the emails as evidence. And tell an adult about them.
- Ask an adult to contact the sender's Internet Service Provider (ISP) by writing abuse@ and then the host, e.g. abuse@hotmail.com
- Never reply to someone you don't know, even if there's an option to unsubscribe'.
- Replying simply confirms your email address as a real one.

Phone calls

- If you get an abusive or silent phone call, don't hang up immediately. Instead, put the phone down and walk away for a few minutes. Then hang up or turn your phone off. Once they realise they can't get you rattled, callers usually get bored and stop bothering you.
- Always tell someone else: a teacher, youth worker, parent/carer. Get them to support you and monitor what's going on.
- Don't give out personal details such as your phone number to just anyone. And never leave your phone lying around.
- When you answer your phone, just say 'hello', not your name. If they ask you to confirm your phone number, ask what number they want and then tell them if they've got the right number or not.
- You can use your voicemail to vet your calls. A lot of mobiles display the caller's number. See if you recognise it. If you don't, let it divert to voicemail instead of answering it. And don't leave your name on your voicemail greeting. You could get an adult to record your greeting. Their voice might stop the caller ringing again.
- Almost all calls nowadays can be traced.
- If you receive calls that scare or trouble you, make a note of the times and dates and report them to the police. You can also report them to the Safeguarding staff at the School. If your mobile can record calls, take the recording too.
- The law is on your side.

The Protection from Harassment Act 1997, the Malicious Communications Act 1988 and Section 43 of the Telecommunications Act 1984 may be used to combat cyber-bullying. People may be fined or sent to prison for up to six months. For more information, see http://wiredsafety.org/gb/stalking/index.html

If you're a parent/carer

- Do not wait for something to happen before you act. Make sure your children understand how to use these technologies safely and know about the risks and consequences of misusing them.
- Make sure they know what to do if they or someone they know are being cyber bullied.
- Encourage your children to talk to you if they have any problems with cyber- bullying. If they do have a problem, contact the School, the mobile network or the Internet Service Provider (ISP) to do something about it.
- Parental control software can limit who your children send emails to and who they receive them from. It can also block access to some chat rooms.
- Moderated chat rooms are supervised by trained adults. Your Internet service provider will tell you whether they provide moderated chat services.
- Visit www.thinkuknow.co.uk/parents for more information on Internet safety.
- Remember, you can do something about it!

Appendix 6: Glossary of cyber security terminology

These key terms will help you to understand the common forms of cyber attack and the measures the school will put in place. They're from the National Cyber Security Centre (NCSC) glossary.

TERM	DEFINITION
Antivirus	Software designed to detect, stop and remove malicious software and viruses.
Cloud	Where you can store and access your resources (including data and software) via the internet, instead of locally on physical devices.
Cyber attack	An attempt to access, damage or disrupt your computer systems, networks or devices maliciously.
Cyber incident	Where the security of your system or service has been breached.
Cyber security	The protection of your devices, services and networks (and the information they contain) from theft or damage.
Download attack	Where malicious software or a virus is downloaded unintentionally onto a device without the user's knowledge or consent.
Firewall	Hardware or software that uses a defined rule set to constrain network traffic – this is to prevent unauthorised access to or from a network.
Hacker	Someone with some computer skills who uses them to break into computers, systems and networks.
Malware	Malicious software. This includes viruses, trojans or any code or content that can adversely impact individuals or organisations.
Patching	Updating firmware or software to improve security and/or enhance functionality.
Pentest	Short for penetration test. This is an authorised test of a computer network or system to look for security weaknesses.

Phishing	Untargeted, mass emails sent to many people asking for sensitive information (like bank details) or encouraging them to visit a fake website.
Ransomware	Malicious software that stops you from using your data or systems until you make a payment.
Social engineering	Manipulating people into giving information or carrying out specific actions that an attacker can use.
Spear-phishing	A more targeted form of phishing where an email is designed to look like it's from a person the recipient knows and/or trusts.
Trojan	A type of malware/virus designed to look like legitimate software that can be used to hack a victim's computer.
Two-factor/multi-factor authentication	Using 2 or more different components to verify a user's identity.
Virus	Programs designed to self-replicate and infect legitimate software programs or systems.
Virtual Private Network (VPN)	An encrypted network which allows remote users to connect securely.
Whaling	Highly targeted phishing attacks (where emails are made to look legitimate) aimed at senior executives.