PHOENIX BAY

E-SAFETY POLICY
SOCIAL MEDIA AND MOBILE PHONE POLICY

Policy Number	**V1**
Date Created	**July 2021**
Owner	**Principal**
Date of Next Review	**July 2022**

Document History

Version	Comments/amendments	Name	Date
1.0	Issue	Ross Banks	July 2021

Contents:

1. Introduction

This policy applies to all members of the school community (including staff, students / students, volunteers, Parents / Carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of the school. It is important for staff to be regularly briefed on new updates.

The Education and Inspections Act 2006 empowers Principals to such extent as is reasonable, to regulate the behaviour of students / students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix for template policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour and Relationship Policy.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform Parents / Carers of incidents of inappropriate e-safety behaviour that take place out of school.

Our school aims to:

- Have robust processes in place to ensure the online safety of students, staff, volunteers and Directors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department'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 students' electronic devices where they believe there is a 'good reason' to do so.

Any searching of students will be carried out in line with the DfE's latest guidance on screening, searching and confiscation. Any complaints about searching for or deleting inappropriate images or files on students' electronic devices will be dealt with through the school complaints procedure.

Acceptable use of the internet in school
All students, Parents/Carers, staff, volunteers and Directors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 and 2). 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.

Educating students about online safety
Students will be taught about online safety as part of the curriculum.
In Key Stage 1, students will be taught to:

- Use technology safety and respectfully, keeping personal information private.
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

2. Key Stages

Students in Key stage 2 will be taught to:

- Use technology, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

Students in Key stage 3 will be taught to:

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

Students 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:

- The use of social media and the internet will also be covered in other subjects where relevant
- The school will use assemblies to raise students' awareness of the dangers that can be encountered online and may invite speakers to talk to students about this
- The Principal will notify Parents of specific relevant issues in a timely fashion

3. Educating Parents about online safety

- The school will raise Parents' awareness of internet safety in letters or other communications home, and information via our website. This policy will be shared with Parents.
- Online safety will also be covered during Parents' evenings.
- If Parents/Carers have any queries or concerns in relation to online safety, these should be raised in the first incident to DSL.

We will monitor the websites visited by students, staff, volunteers, Directors and visitors (where relevant) to ensure they comply with the above.

Staff using work devices outside school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 2.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted.
If staff have any concerns over the security of their device, they must seek advice from the Principal. Work devices must be used solely for work activities.

How the school will respond to issues of misuse

Where a student misuses the school's ICT systems or internet, we will follow the procedures set out in the Behaviour and Relationship policy. 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 disciplinary procedures. 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.

4. 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).

The 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 about online safety at regular intervals, and at least annually.

Directors 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.
More information about safeguarding training is set out in our Safeguarding and Child Protection policy.

5. Social Media

Phoenix Bay School recognises that many staff, Directors, Parents, Carers, and students have a personal use for the internet and that they may participate in social networking on social media websites such as Facebook, Twitter, Instagram, etc.

Whilst staff, Directors, Parents and Carers are free to use the internet in this way, they must ensure that they do not breach the law or disclose Phoenix Bay School's confidential information, breach copyright, defame the school, its staff, Directors, Parents, Carers and students. They must not disclose personal data or information about any individual that could breach the Data Protection Act 2018 (GDPR) or Phoenix Bay School's E-Safety policy. They should keep completely confidential, any information regarding the children, their families or other staff which is learned through the school.

The purpose of this policy is to outline the responsibilities of staff, Directors, Parents, and Carers who are engaging in social media, networking websites, blogs and using online dating websites.

Personal websites and blogs
The following guidelines apply:

- Staff, Directors, Parents, and Carers must not disclose any information that is confidential to the school or any third party that has disclosed information to the school
- Staff, Directors, Parents and Carers should not link any personal websites, social networking site to the school's website.
- If a member of staff, Directors, parent or Carers is asked to contribute to an official weblog connected to the school, then special rules will apply, and they will be told in detail how to operate and what to write.
- Phoenix Bay school will not tolerate criticisms through social medial. If a member of staff feel aggrieved then they must follow the procedures outline in the Complaints Policy.

Social networking sites
The school respects a member of staff's right to a private life. However, the school must also ensure that confidentiality and its reputation are protected.
The school expects all staff, Directors, Parents, and Carers to:

- Ensure that they do not conduct themselves in a way that is detrimental to the school
- Take care not to allow their interaction on these websites to damage working relationships between members of staff and clients of the school

Important considerations
Staff, Directors, Parents, and Carers should be aware that social networking websites are a public forum, particularly if they are part of a 'network'. Staff, Directors, Parents, and Carers should not assume that their entries on any website will remain private.

When using social media, networking and online dating websites, staff, Directors, Parents, and Carers should follow these guidelines:

- Staff should not except friend requests from Phoenix Bay students, Parents or Carers under any circumstances. Where relationships are already established, staff should proceed with caution, being fully aware of the social media guidelines and the code of conduct.
- Staff should increase their privacy settings wherever available.
- Staff should not share personal conversations
- Staff should behave respectfully and should not engage in topics that may be considered objectionable or inflammatory such as politics or religion.
  Do not defame (libel) anyone. A member of staff, director, parent or carer who makes a defamatory statement that is published on the internet may be legally liable for any damage to the reputation of the individual concerned.
- Do not post material that is abusive, defamatory, sexist, racist or that could be interpreted as harassment or bullying.

Personal use of the internet
Phoenix Bay School does not allow personal use of the internet during work hours on school devices. All personal devices should be stored safely in the staffroom and only accessed during a recognised break.

Examining electronic devices
School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.
When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of students will be carried out in line with the DfE's latest guidance on screening, searching and confiscation. Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

Disciplinary action
If necessary, action will be taken against any member of staff, director, parent, or carer who is found to have breached this Policy.

Security and identity theft
Staff, Directors, Parents and Carers must be security conscious and should stay proactive, taking steps to protect themselves from identity theft, for example by restricting the amount of personal information that they give out. Social networking websites allow people to post detailed personal information such as date of birth, place of birth and, for example, favourite football team which can form the basis of security questions and passwords.

6. Mobile Phones

Students using mobile devices in school

Students may bring mobile devices into school but are handed into staff at the start of the day.
Any use of mobile devices in school by students must be in line with the acceptable use agreement (see appendix 1).
Any breach of the acceptable use agreement by a student may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

Staff & Mobile Phones

During their working school day staff mobile phones should only be used when in a staff only area. Mobile phones should be switched off and stored in a safe place not accessible by staff or children, especially during lesson. The school will not take responsibility for any items that are lost or stolen.

Where a phone call is expected upon the mobile phone, staff are advised to leave it with staff in the admin office. They will be informed if the call is received. Staff are advised to give the school telephone number to be contacted upon during the school day.

School excursions /residentials – staff are required to take a mobile phone to ensure they have full contact with school in case of an emergency. In such cases staff are expected to carry the phone upon themselves and if appropriate ensure it is not on silent. Staff are reminded of policy to not use for any other reason other than in communication with school or in an emergency.
Strictly no photos should be taken of the children or activities. A school camera should be used for any photos.

Staff should never contact students or Parents from their own personal mobile phone or give them their mobile number to students or Parents. If a member of staff needs to make telephone contact with a parent or student, a school telephone should be used.
With regards to cameral mobile phones, a member of staff should never use their phone to photograph a student(s). or allow themselves to be photographed by a student(s).

This guidance should be seen as a safeguard for members of staff. Staff should understand that failure to comply with this policy is likely to result in the enforcement of our whistleblowing policy and associated procedures.

Staff work mobiles

The use of a designated work mobile is allowed as:

- An essential part of the emergency toolkit which is taken on off-site trips.
- A communication aid, enabling text, email messages and calls to be made and received from Parents/Carers and other professionals.
- A back-up facility should problems be experienced with the landline – or where contact needs to be made outside of work hours.
- As a safety measure for staff with an outreach function in their job role.
- Staff who are permitted to use a work mobile phone should try not to use them in the presence of students and make sure they can't be over-heard when making confidential calls.

7. Cyber-Bulling

Definition

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

Preventing and addressing cyber-bullying

- To help prevent cyber bullying, we will ensure that students understand what it is and what to do if they become aware of it happening to others or themselves. We will ensure that students 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 students, explaining the reasons why it occurs, the forms it may take and what the consequences can be.
- Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes during SEMH lessons, (PSHE) education, and other subjects where appropriate.
- All staff, Directors and volunteers (where appropriate) receive training on cyber-bullying, it's impact and ways to support students as part of the safeguarding training.
- 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.

8. Acceptable Use Agreement

Students should be helped to understand the need for the student Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.

Staff should act as good role models in their use of digital technologies the internet and mobile devices in lessons where internet use is pre-planned, it is best practice that students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Where students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Students should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.

Nb. additional duties for schools/academies under the Counter Terrorism and Securities Act 2015 which requires schools to ensure that children are safe from terrorist and extremist material on the internet.

Appendices:

A. Student Acceptable Use Policy Agreement

This is how we stay safe when we use computers:

I will ask a teacher or suitable adult if I want to use the computers

I will only use activities that a teacher or suitable adult has told or allowed me to use

I will take care of the computer and other equipment

I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong.

I will tell a teacher or suitable adult if I see something that upsets me on the screen.

I know that if I break the rules I might not be allowed to use a computer.

Signed (child):…….. Date: .....

Signed (parent): …….. Date .....

B. Parent / Carer Acceptable Use Agreement

Digital technologies have become integral to the lives of children and young people, both within schools and outside school.

These technologies provide powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning.

Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that Parents and Carers are aware of the importance of e-safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that students will have good access to digital technologies to enhance their learning and will, in return, expect the students to agree to be responsible users.

A copy of the student Acceptable Use Policy is attached to this permission form, so that Parents / Carers will be aware of the school expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

Parent/Carer Acceptable Use Agreement
Permission Form

Parent/Carers Name .....

Student Name.....

As the parent / carer of the above student(s), I give permission for my son/daughter to have access to the internet and to ICT systems at school.

I know that my son/daughter has signed an Acceptable Use Agreement and has received, or will receive, E-safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's/daughter's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Agreement.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's E-safety.

Parent/ Carer signature .....

Date .....

C. Use of Digital/Video Images

The use of digital / video images plays an important part in learning activities. Pupils and members of staff may use digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons.

Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media.

The school will comply with the General Data Protection Regulation and request Parents / Carers permission before taking images of members of the school. We will also ensure that when images are published that the young people cannot be identified by the use of their names.

Parents / Carers are welcome to take videos and digital images of their children at school events for their own personal use. To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should Parents / Carers comment on any activities involving other students / pupils in the digital / video images.

Parents / Carers are requested to sign the permission form below to allow the school to take and use images of their children

Video Images Permission Form

Parent/Carers Name .....

Student Name .....

As the parent / carer of the above student, I agree to the school taking and using digital / video images of my child / children. I understand that the images will only be used to support learning activities. **Yes/No**

As the parent / carer of the above student / pupil, I agree to the school taking and using digital / video images of my child / children. I understand that the images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media. **Yes/No**

I agree that if I take digital or video images at, or of, – school events which include images of children, other than my own, I will abide by these guidelines in my use of these images. **Yes/No**

You may withdraw any consents given at any time by contacting the School Office and informing them of your decision.

Parent / Carer Signed .....

Date .....

Author	Ross Banks
Document Title	E-Safety, Social Media & Mobile Phone Policy
Date Reviewed	July 2021
Next Review Date	July 2022