Poole Grammar School E-Safety Policy for All Staff

Issued: September 2018

E-Safety Policy

The school has a duty to safeguard and promote the well-being of the young people in its charge. In fulfilling this duty the school provides a range of education avenues including some which use or promote the use of technology. This gives rise to a need to clarify:

a) How all teaching and support staff should use technology appropriately in circumstances where contact with young people can occur.

b) How we develop the capacity of the young people in our charge and the adults who work with them in school to use technology safely and appropriately.

c) Current potential threats to all young people which are most likely to emanate from their use of technology.

Purpose

To enable students and all staff to benefit from technology whilst remaining safe and behaving lawfully.

Who must comply with the policy?

All school staff must comply with this policy. Contact means face-to-face contact and contact through any sort of technology.

When does this policy apply?

This policy applies at all times (52 weeks a year) inside and outside of school and relates to all school staff who work with students and their parents / carers at Poole Grammar School.

What is the policy?

Principles

School staff are in a position of trust. They must avoid any conduct which would lead any reasonable person to question their motivation and intentions.

Staff must work according to the Government 'Guidance for safer working practice for adults who work with children and young people' – available on the Safeguarding area of Moodle for reference.

Staff should also read this document in conjunction with the latest version of Keeping Children Safe in Education:

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/707688/Keeping_Children_Safe_in_Education_-_Part_1_-_September_2018.pdf

and in the context of the GDPR training received in respect of the legislation introduced May 2018.

Staff should be able to use the internet, and related communications and technologies, appropriately and safely.

To do this the School will:

- Promote and procure technology that helps to support safe and legal working.
- Train staff appropriately. General full staff training given annually and updates provided throughout the year. Additionally specific safeguarding, teaching and IT support staff attend SSCT E-Safety training courses and E-safety Champion training attended annually. Full SSCT training given to staff at the start of the 2017-18 academic year. Training for the GDPR legislation provided to all staff in the run up to 25th May 2018.
- Monitor staff activity where appropriate through the school network by the Network Team. Any concerns are relayed to the Designated Safeguarding Lead in the first instance.
- Identify an E- Safety Champion. From September 2018 this will be Mr Mark Hayward. In his role as PHSE Co-ordinator he will be the professional with a role to promote E- Safety. Liaise with the SSCT and work with students in this area. Any safeguarding issues related to misuse of technology will be co-ordinated with the DSL or one of their deputies.

The school believes that young people should be empowered to access appropriate information via technology to develop their learning, support communication and facilitate social interaction.

To do this the school will promote learning about safe and legal use of technology for students plus their parents and carers. This is done through the ICT curriculum, the PHSE programme and through bespoke presentations to Main School year groups and parents annually by the Police Safe Schools and Communities Team. Safer Internet Day is promoted each year. Copies of the Vodafone Digital Parenting Guide are issued to Year 7 parents when their son joins the school.

The school expects that where staff may have concerns about inappropriate use of technology involving students they must report this, immediately and confidentially, directly to one of the designated members of staff in accordance with the normal child protection procedures.

Communication between staff and students – protocol

Since April 2017, it has been a criminal offence for an adult (18 and over) to send a sexual communication to a child under 18. Professionals should report incidents they believe may fall under this offence to the DSL or by making a crime report on the Dorset Police website https://www.dorset.police.uk/do-it-online/full-crime-report/.

Communication with students involving digital technology must be carried out in a professional manner using the recognised school systems rather than any private context that will then be transparent in the event of any potential challenge. This means that:

i. The communication will be carried out using school controlled systems and accounts rather than private ones. Where publically available platforms are used (such as social media services) specific accounts must be setup for official purposes and only with approval by the school management. Privacy settings for these should be configured such that identities, personal information and the ability to make unsolicited contact are secured.

ii. The content of communications will relate solely to official matters such as learning, impartial advice and guidance, pastoral support or handling practical arrangements for official activities such as school fixtures or trips. Any such form of communication will be with the knowledge and consent of the parent/carer.

iii. Staff should take great care in their communications with students, past and present so as to avoid any possible misinterpretation of their motives or any behaviour which could be construed as grooming.

iv. There is to be strictly no contact with any student on roll or a parent via the professional's personal use of social media sites e.g. Facebook or personal communication systems e.g a private e-mail account or texting on a personal mobile phone.

v. Should a current student be friends with a member of staff's child and/or there be contact between the member of staff concerned and the other parent(s) in a social context, this should be flagged up to the line manager.

vi. Personal information of staff such as private contact details including phone numbers and social media accounts must not be shared with pupils on roll at any time.

vii. Staff should not request personal information from students or parents/carers other than that which is required for clear official purposes.

viii. Where staff have access to the proxy this is understood to be wholly to aid in their professional work and any attempt to access inappropriate material will be deemed a disciplinary matter.

The scope of "communication" includes still and moving images / graphics / audio content as well as text on mobile phones, posts or comments on social media sites and e-mail. **Staff should not use personal devices in any area of the school where students are present – classroom, around the public areas of the school buildings or in the grounds during recreational times.**

The use of digital images

Parental permission is sought and preserved for reference on the student record card for the taking and use of images of their son on his entry to the school. Those taking pictures should establish whether this permission has been given prior to publishing photographs, and then only in the places outlined in (iv) below.

i. Permission must be sought from parents of students up to 13 years of age and thereafter from the students themselves for use of their image in a situation where they can be recognised.

ii. Care must be taken when capturing digital images that young people are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute. Avoid taking photographs in one to one situations.

iii. The full names of students will not be used without express permission and only where appropriate on the school website, blog, or published article such as the school magazine, particularly in association with photographs. Close consideration should be given to media coverage to ensure that there is no inappropriate release of information about students.

iv. Digital images made by staff must be done so using equipment specifically supplied by or approved by the school. Storage of these images must be on school equipment for transparent educational reasons that would withstand challenge should the motivation of a member of staff be brought into question. **Staff should not transport images on mobile devices or memory sticks which could be easily misplaced.**

Access to Inappropriate Images and Internet Usage

i. There are no circumstances that will justify adults possessing indecent images of children. Adults who access and possess links to such websites will be viewed as a significant and potential threat to children. Accessing, making and storing indecent images of children on the internet is illegal. This will lead to criminal investigation and the individual being barred from working with children and young people, if proven.

ii. Adults should not use equipment belonging to school to access adult pornography; neither should personal equipment containing these images or links to them be brought into the workplace. To do so will raise serious concerns about the suitability of the adult to continue to work with children.

iii. Adults should ensure that pupils are not exposed to any inappropriate images or web links. The school will act to ensure that internet equipment used by children have the appropriate controls with regards to access. e.g. filtering systems will be in place & passwords should be kept confidential.

iv. Where indecent images of children or other unsuitable material are found, the Police and Local Authority Designated Officer (LADO) will immediately be informed. Staff should not attempt to investigate the matter or evaluate the material themselves.

For managing allegations against staff the guidance on the LSCB web site: www.bournemouth-poolelscb.org.uk/interagency_safeguarding_procedures/pictures/content296/chapter_3.9_managing_allegations_against_people_who_work_with_children_updated_oct_11.pdf will be followed. See additional note on Youth Produced Sexual Imagery below.

Teaching and Support Staff private use of digital media

i. In their private use of digital media (such as social networking sites) staff must protect their professional reputation and that of the school. This must be achieved through the judicious application of privacy settings so that communications remain private from children and young people / parents and carers and through the avoidance of rhetoric that might cause reputational damage to individuals or the institution. At all times think before you post as to whether what you have written is acceptable to your reputation as a professional now and in the future.

ii. All staff must not solicit or accept "friend / contact / circle / follow" - type connections to private accounts with any young people for whom they have any professional responsibility. Due care must be taken if undertaking any electronic communication with parents & carers for any reason. Social contact should be limited to personal friends and any such relationship made explicitly clear to the line manager.

iii. Staff must not engage in any communication which could bring the school into disrepute which includes postings made on their own or others' personal sites, blogs etc. Staff must be mindful of confidentiality and data protection. If a staff member becomes aware that they have posted a comment or have witnessed one which may bring themselves or the school into disrepute or breach data protection they must bring this to the attention of the Headteacher or Designated Safeguarding Lead immediately.

iv. At all times staff must be respectful of others, not engaging in any communication which could be deemed as breaking the law regarding discrimination or offensive behaviour. They must never use social media to negatively comment on, bully or harass another adult, colleague or write anything in respect of any young person with whom they have professional contact. Staff should be aware of the concept of 'digital footprint' whereby anything posted could potentially compromise their professional integrity now or in future.

Students' use of technology

i. Staff who directly supervise students must ensure that use of the internet through official infrastructure is monitored. The level of this supervision / monitoring should be age appropriate ie this may be different for a Year 7 to a Year 13. Guidance should be sought if uncertain about the appropriateness of any particular content that is shown to or used by pupils of a given age. A useful guide is the Brook Traffic Light Tool:

https://www.brook.org.uk/our-work/the-sexual-behaviours-traffic-light-tool?utm_source=brook&utm_campaign=traffic-light-tool-dec&utm_medium=homepage-banner

ii. Age appropriate safety mechanisms such as content filtering must be employed for students accessing the internet via school infrastructure. Breaches of these safety mechanisms (for example through the use of proxy websites) must always be challenged. Staff should be vigilant with respect to students accessing inappropriate material in school via personal devices and challenge them if necessary. Use of such devices must at all times be in line with the school regulations.

iii. Staff must ensure that any films or material they show to children or sites they ask children to access to find information are age appropriate.

iv. It is the responsibility of staff to ensure as far as possible that young people are not, while in their direct care, involved in plagiarism and copyright infringement, illegal downloading of copyright files, hacking, viruses or other breaches of system security.

v. All staff in contact with pupils have a responsibility to advise about and encourage E-Safety and good behaviour in relation to personal online activity as well as that in the setting e.g. avoiding contact with strangers which may lead to grooming, access of age appropriate content, use of privacy settings in social media, risks of online gaming, cyber-bullying, respect for copyright and the security of personal information. This will be aided through the delivery of a planned curriculum of digital literacy and E-safety. They should advise against excessive use of any technology in contexts such as gaming which impacts on social and emotional development.

vi. Even where contact is brief, informal and unstructured, good behaviours online should be at all times acknowledged and inappropriate behaviours challenged.

vii. The planned curriculum for E-Safety awareness is delivered through the ICT department and in specific work from the SSCT in terms of the E-Safety Day across the school. This also includes involvement of parents and carers through contact with home in terms of information and advice given out plus the provision of an E-Safety Parents Evening. Hard copies of the Vodafone Digital Parenting Guide have been issued to all parents of the new Year 7 2018.

viii. Policies and procedures for the use of technology are shared and routinely refreshed through posters, lessons, pastoral work, staff training and induction procedures, etc. They are also shared with parents and carers through the school diary and communications through the year for events such as Anti-Bullying Week and Safer Internet Day.

ix. The Acceptable User Policy is explicit in the diary where it is signed by the pupil and their parent/carer. Different mobile phone rules apply to students in Years 7 & 8 whereby internet-accessible devices and those with a capability to take photographs or videos are not permitted. This policy is clearly indicated in the school diary.

x. Any form of bullying, including cyber-bullying, is not acceptable and there will be sanctions in place for any young person who engages in cyber-bullying. These form part of the Anti-Bullying and Behaviour Policy. Pupils are encouraged to report unacceptable behaviour online to a parent, teacher or by using the CEOP reporting button on the ThinkyouKnow website. For significant events or concerns the Safe Schools and Communities team will be contacted.

Enforcement

Breaches of this policy will fall into the following categories:

- Illegal acts by staff – Escalated to Police/LADOs/Children's Social Care.

- Breaches of policy – Following investigation by LADOs / Children's Social Care/HR/Data protection as appropriate, these will be addressed the Headteacher and Governing Body in accordance with the school's disciplinary procedures and GDPR regulations.

Other relevant Guidance

Poole Grammar School Child Protection and Safeguarding Policy & Procedures booklet incorporating 'Protecting yourself as a Professional – Advice for Staff, Student-Staff Communication Protocol' is issued to all staff and should be held available for their reference.

Protecting Your Professional Identity presentation – on Safeguarding area of Moodle for reference.

All Safeguarding documents should be read in conjunction with the Part 1 of Keeping Children Safe in Education September 2018 which has been issued to all staff and is available on Moodle for reference.

The Prevent Duty

Protecting young people from potential extremism and radicalisation is now a key Safeguarding area. This is most likely to occur through the use of any form of digital media. Staff should therefore be aware at all times with regard to direct usage of, and discussion about, any sort of online material of this type by young people. Reference should be made to the document:

https://www.gov.uk/government/publications/protecting-children-from-radicalisation-the-prevent-duty

All staff have undertaken online training on this topic and the records are held by the Head's PA. Mr Andy Baker as Headteacher has undertaken WRAP training and is the Designated Lead for Prevent for Poole Grammar. Further training and updates from the Police were received July 2018.

Youth Produced Sexual Imagery

A particular focus in this regard is **Youth Produced Sexual Imagery** (previously known as 'sexting'). If you suspect at any time that a student has created, distributed or received a sexualised image or video on a device then please relay this concern immediately to the Designated Safeguarding Lead. If you think that the mobile device of a student may contain inappropriate images or content then the law states:

Headteachers and staff authorised by them have a statutory power to search students or their possessions, without consent, where they have reasonable grounds for suspecting that a student may have a prohibited item banned by the school rules.

Do not attempt to view any image yourself and never print, copy or share any sort of image – there are strict procedures in place regarding how such incidents will be dealt with and this will be in consultation with the Police where necessary. YPSI is a crime and, where investigated by the Police such incidents are now recorded as an 'Outcome 21'. Further details are available at:

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/609874/6_2939_SP_NCA_Sexting_In_Schools_FINAL_Update_Jan17.pdf

Child Sexual Exploitation

Linked to, and including YPSI, staff should be aware of the potential of young people being exploited through the various forms of digital media. Again, any form of conversation, attendance pattern or behaviour that causes concern should be reported. Further information found at:

https://www.gov.uk/government/publications/child-sexual-exploitation-definition-and-guide-for-practitioners

Supporting information

http://ceop.police.uk/ For advice and guidance from the Police's Child Exploitation and Online Protection Unit (CEOP).

http://www.swgfl.org.uk/Staying-Safe For E-safety support material from the South West Grid for Learning who provide Internet connectivity to nearly all state schools in the 15 South West local authorities as well as actively managed filtering and monitoring. This includes Standard Acceptable User Policies, bring your own device, advice on clouding etc.

http://www.iwf.org.uk/ Internet Watch Foundation, for the reporting of criminal online content.

http://webarchive.nationalarchives.gov.uk/20100202101002/dcsf.gov.uk/everychildmatters/resources-and-practice/ig00311/ Guidance for safer working practice for adults who work with children and young people – government 2009. Available for reference on Safeguarding area of Moodle

https://parentzone.org.uk/system/files/attachments/Digital%20Parenting%206%20NEW.pdf has excellent advice and information for parents and professionals

Safe Schools and Communities team ssct@dorset.pnn.police.uk 01202 222844. This team provides support if an E-safety incident occurs as well as training for pupils, parents/carers and staff.

K M McDonald

Designated Safeguarding Lead

September 2018

Given the fast-moving nature of the development of technology and its use this policy will be reviewed annually.