E-SAFETY POLICY

PILGRIM
PATHWAYS
SCHOOL

Approved by:	Management Committee	**Date approved:**	1st June 2019
Date reviewed:	June 2018	**Next review due by:**	June 2021
Policy Lead:	Leah Miller, Headteacher	**Ownership:**	Pilgrim PRU Management Committee

Table of Contents

E- Safety Policy

Legislation and guidance that inform this document

● Children Act (2004)
● The safe use of new technologies (Ofsted 2010)
● Working together to safeguard children (Gov.UK 2015)
● Keeping Children Safe in Education (Gov.UK 2016)

Other Pilgrim PRU policies to be read in conjunction with this one

● Code of Conduct for all Staff
● Safeguarding and Child Protection
● Behaviour for Learning
● Anti-bullying
● Data Protection
● Whistleblowing

1. Statement of Intent

Ofsted describes E-safety as a school's ability to protect and educate pupils and staff in their use of technology as well as having appropriate mechanisms in place to intervene and support any incident where appropriate.

Pilgrim PRU is committed to utilising technology to inform and support learning. We seek to embrace new developments that offer improved learning opportunities to students. Equally we are determined to ensure that all Pilgrim PRU students and staff remain safe and free from the dangers implicit in the use of that technology. Our aims are to ensure that:

- students do not access material that may be damaging or disturbing to them;
- students do not access material that might be considered to be politically inflammatory or lead them towards 'extremist' /'terrorist' behaviour;
- students are not subject to cyber-bullying of any sort;
- students do not engage in the posting of any material that might be deemed offensive or threatening (to anyone, but particularly to other members of the Pilgrim PRU community);

- staff are professional in their use of social media and networking sites.

In line with general Pilgrim PRU aims our intentions are that students:

- take responsibility for their online presence and acknowledge / understand that 'virtual' behaviour is akin to real world behaviour with the same rights and responsibilities attached;
- are well prepared for life beyond Pilgrim PRU;
- make informed decisions for themselves.
- in line with school hospital E-safety protocols staff must inform the nurse in charge if a young person has breached the hospital E-safety policy whilst in school.

2. Key Factors within E-Safety

- Online behaviour – understanding what constitutes cyber-bullying and sexting, how to behave safely and with respect for others;
- protecting online reputation – understanding both the risks and rewards of sharing personal information online (digital footprint);
- how to use social networking safely;
- understanding the reliability and validity of online information;
- data security – keeping personal information safe and being aware of viruses and hacking;
- knowing what to do if anything 'bad' happens.

In summary all staff will work to ensure that risk is minimised within the two key 'danger' areas:

- **content** – what students may see or be exposed to (eg spam, misleading adverts, inappropriate sites, exposure to radicalisation);
- **contact** - who students have contact with...
- and that students understand how to **conduct** themselves safely online.

Pilgrim PRU management is acutely aware of its responsibilities under the new 'Protect' guidance (see Safeguarding and Child Protection Policy) and will ensure all staff are trained to reduce the risk of any Pilgrim PRU student accessing material likely to lead to radicalisation, but also that students are encouraged to discuss openly any concerns or worries they have regarding radicalisation.

3. Specific Responsibilities

The Management Committee will ensure that:

Appropriate policy is in place and all practice is in line with policy, so that students are able to use technology in an informed and safe fashion to structure and support their learning.

In order to fulfil that role the Management Committee will:

- ensure this e-safety policy is maintained and updated;
- ensure each centre has an agreement (generated between students and staff) concerning the appropriate use of technology;
- ensure compliance with regulations;
- provide (either directly or through access to appropriate providers) high quality training for staff;
- provide clear guidelines for students regarding the consequences of online bullying and inappropriate use of technology;

- ensure all hospital and school staff offer clear, open lines of communication through which students are able to report any incidents of concern;
- ensure procedures are in place for responding to safety incidents and reducing the likelihood of their recurrence;
- ensure Pilgrim PRU staff provide training and support to students to help them become 'digitally responsible' and to stay safe online;
- ensure that Pilgrim PRU staff monitor and filter online access to help keep students safe and reduce the likelihood of harmful experiences on line
- ensure Pilgrim PRU staff engage with parents to help them put e-safety procedures in place at home.

4. Teachers in Charge

Each Teacher in Charge is responsible for ensuring that practice in their centre complies with policy.

Teachers and support staff are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current Pilgrim PRU e-safety policy and practices;
- they have read and signed the Pilgrim PRU statement on responsible internet use.
- they report any suspected misuse of technology or problems to their coordinator (or to a member of 'Group' should that misuse be by the coordinator);
- all digital communications with students or their parents are only carried out using official school systems;
- e-safety issues are embedded in all aspects of the curriculum;
- teacher use of Google drive for keeping student records and information must be password protected and information must not be shared with outside agencies.
- students are involved in the development of guidelines for acceptable technology use and that they subsequently follow those guidelines;
- students understand and uphold copyright regulations;
- students monitor the use of digital technologies, mobile devices, cameras etc. in lessons and during other school activities and implement policies with regard to these devices;
- students are helped to access appropriate sites only and, if inappropriate material is accessed, processes to ensure that the likelihood of repeated access is minimised are followed.

As a working professional unit, teachers and support staff must ensure that e-safety is embedded in general practice and taught as a core cross-curricular theme.

The designated person for child protection (Amanda Morris-Drake) within each centre should be trained in e-safety issues and be aware of the potential for serious child protection / safeguarding issues that may arise from arise from:

- sharing of personal data;
- access to illegal or inappropriate materials;
- inappropriate online contact with adults or strangers;
- potential or actual incidents of grooming;
- cyber-bullying.

· NB It is important to emphasise that these are child protection issues, not technical issues. The technology simply provides additional means for child protection issues to develop.

Students:

- are responsible for using technology systems within centres according to the 'acceptable use' guidelines;

- should uphold copyright regulations;
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;
- will be expected to be involved in the development of, and policies on the use of, mobile devices, digital cameras, and other technology;
- should be aware of Pilgrim PRU policy re cyber-bullying;
- should understand the importance of adopting good e-safety practice when using digital technologies out of school.

Parents: *(NB 'parents' is understood to include carers)***:**

Parents play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Pilgrim PRU staff will take every opportunity to help parents understand these issues by including E-safety information in the parent information pack and on the website. Parents will be encouraged to support Pilgrim PRU staff in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events;
- access to parents' sections of the website and other online sites (such as ParentView);
- their children's personal devices whilst attending a centre or engaging with online learning.

Use of Digital / Video Images:

Staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular students should come to recognise the risks attached to publishing their own images on the internet (such as social networking sites).

Equally students may take photographs of their peers, but they must not take, use, share, publish, or distribute images of others without their permission.

The Pilgrim PRU discourage taking photos of students but Staff may take photographs of students when engaged in school activities, but due care should be taken regarding the following:

- students should be appropriately dressed;
- written permission must be obtained from parents / carers before photographs are used on the Pilgrim PRU website or in other information / publicity materials e.g. newsletters, fliers;
- students' full names should not be posted on a website or blog or within publicity materials when associated with photographs.

NB Staff must never circulate by email or text, or post on social media sites, photographs of students taken at a centre or elsewhere (for instance, on residential trips). Any such action will lead to disciplinary action and, possibly, dismissal.

'Sexting':

In the UK, it is against the law to share or distribute explicit images of anyone under the age of 18 - even if the person sharing them is the person in the photo. If caught, students can face police cautions or even arrest, based on the nature of the imagery, which can lead to a criminal record and later failings of DBS checks. Staff will work to ensure that all students know the risks of sending X-rated photos from a personal, emotional and criminal perspective. However an agreement currently exists between the National Police Chiefs Council (formerly ACPO) and the Crown Prosecution Service that advises police forces NOT to prosecute young people sexting unless there are very good reasons to do so.

If it comes to a member of staff's attention that students are exchanging explicit images across social media - whether invited or not - it is crucial that the situation is dealt with thoroughly and sensitively. Regardless of whether the sharing happens at home or on Pilgrim PRU premises, if it involves Pilgrim PRU students, and is affecting their work or wellbeing, it should be treated as a school matter, and the involved parties should be approached for advice. We are 'allowed' to deal with such matters internally, but will seek advice from the LSCB when deemed necessary. Referrals to the police will only be made if advice from the LSCB is that this is the appropriate course of action.

Staff Postings:

School staff must ensure that:

- no reference is made on social media to students, parents / carers or school staff ;
- they do not engage in online discussion on personal matters relating to members of the school community;
- personal opinions expressed online are not attributed to Pilgrim Pru;
- security settings on their own personal social media profiles are such that students cannot access personal information that is posted there.

ICT support staff and external contractors:

- CCC ICT support staff and technicians are responsible for maintaining the school's networking, IT infrastructure and hardware. They need to ensure that the school system, particularly file- sharing and access to the internet is secure. They need to further ensure that all reasonable steps have been taken to ensure that systems are not open to abuse or unauthorised external access.
- Support staff also need to maintain and enforce the schools' password policy and monitor and maintain internet filtering.

Management Committee:

- The Management committee should access the online E-safety training that is available through the E-Safety support package. The head will send out E-safety training links to members of the management committee on a regular basis.

How will the Pilgrim PRU provide E-safety education:

- As part of their induction all students should undertake the online E-safety training.
- All staff will need to complete online safety training as part of their induction.
- E-safety is taught as part of the PSHE curriculum **Pilgrim PRU staff responsible internet use**

Covers use of digital technologies in the service: i.e email, Internet, Intranet and network resources, learning platform, software, equipment and systems including iPads.

We encourage staff to use and explore ICT to enhance their skills, increase subject knowledge and to widen students' access to learning opportunities.

- I will only use the school's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the Head and PRU Management Committee.
- I will not reveal my password(s) to anyone.
- I will follow 'good practice' advice in the creation and use of my password. If my password is compromised, I will ensure I will change it. I will not use anyone else's password if they reveal it to me and I will advise them to change it.
- I will not allow unauthorised individuals to access email / Internet / intranet / network, or other school systems.
- I will ensure all documents, data etc., are saved, accessed and deleted in accordance with the school's network and data security and confidentiality protocols.
- I will not engage in any online activity that may compromise my professional responsibilities.

- I will only use the approved, secure email system(s) for any school business.
- I will only use the approved school email or other school approved communication systems with pupils or parents/carers, and only communicate with them on appropriate school business.
- I will not browse, download or send material that could be considered offensive to colleagues.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the appropriate line manager / school named contact as outlines in the service e-safety policy.
- I will not download any software or resources from the Internet that can compromise the network, or are not adequately licensed.
- I will not publish or distribute work that is protected by copyright.
- I will not connect a computer, laptop or other device (including USB flash drive), to the network / Internet that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the school's recommended anti-virus, firewall and other ICT 'defence' systems.
- I will not use personal digital cameras or camera phones for taking and transferring images of pupils or staff without permission and will not store images at home without permission.
- I will ensure that any private social networking sites / blogs etc that I create or actively contribute to are not confused with my professional role.
- I agree and accept that any computer, laptop or iPad loaned to me by the service, is provided solely to support my professional responsibilities and that I will notify the service of any 'significant personal use' as defined by HM Revenue & Customs.
- I will access service resources remotely (such as from home) only through the service agreed methods and follow e-security protocols to access and interact with those materials.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow service data security protocols when using any such data at any location.
- I will embed the service's e-safety curriculum into my teaching.
- I will alert the service's named designated member of staff for safeguarding Amanda Morris-Drake) if I feel the behaviour of any pupil may be a cause for concern.
- I understand that it is my duty to support a whole-service safeguarding approach and will report any behaviour (of other staff or pupils), which I believe may be inappropriate or concerning in any way, to a member of the head of the Pilgrim PRU.
- I understand that failure to comply with this agreement could lead to disciplinary action.

User Signature:

I agree to abide by all the points above.

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent e-safety policies.

I wish to have an email account; be connected to the Internet; be able to use the service's ICT resources, database and systems.