Online Safety Policy

Applies to:

- The whole school along with all activities provided by the school, including those outside normal school hours;
- All members of the school community, including staff, pupils, volunteers, parents and visitors, who have access to and are users of the school IT systems'
- All staff (teaching and support), governors and volunteers working in the school.

This Online Safety Policy and our Acceptable Use of IT Policy cover both fixed and mobile internet devices provided by the school such as PCs, laptops, webcams, tablets, whiteboards, digital video equipment, etc., as well as all devices owned by pupils and staff brought onto school premises such as personal laptops, tablets, wearable technology, e.g. smart phones, watches, etc. They also cover when pupils are going online in the home environment, for example when accessing remote learning.

We aim to ensure that every pupil in our care is safe, and the same principles apply to the digital world as apply to the real world. IT and online communications provide unrivalled opportunities for enhanced learning in addition to traditional methods, but also pose greater and more subtle risks to young people. Our pupils are therefore taught how to stay safe in the online environment and how to mitigate risks, including, but not limited to, the risk of identity theft, bullying, harassment, grooming, stalking, abuse and radicalisation.

Related Documents

- Anti-Bullying Policy
- Behaviour Policy
- Health and Safety, Risk Assessment and Welfare Policy
- Data Protection Policy
- Remote Teaching & Learning Policy
- Safeguarding Policy
- Staff Code of Conduct
- Acceptable Use of IT Policies (Pupils, and Staff and Governors)

This Policy Takes into Account:

- DfE statutory guidance 'Keeping Children Safe in Education' 2023;
- DfE guidance 'Teaching online safety in schools', June 2019, which outlines how schools can ensure their pupils understand how to stay safe and behave online as part of existing curriculum requirements
- UKCIS 'Education for a Connected Word' Framework, June 2020 : Education for a Connected World - GOV.UK (www.gov.uk)
- DfE advice for schools: 'Sharing nudes and semi-nudes, advice for education settings working with children and young people': Sharing nudes and semi-nudes: advice for education settings working with children and young people - GOV.UK (www.gov.uk)

Availability:

This policy is made available to parents, staff and pupils in the following ways: via the school website, within the Parent Policies Folder in the Reception area, and on request a copy may be obtained from the school office.

Monitoring and Review:

This policy is subject to continuous monitoring, refinement and audit by the Principal, and is reviewed at least annually.

Signed:

Amy Cavilla
Principal
September 2024

1. Introduction

1.1. It is essential that children are safeguarded from potentially harmful and inappropriate online material. Radnor House Twickenham's whole school approach to online safety empowers the school to protect and educate pupils and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate.

1.2. It is recognised by the school that the use of technology presents particular challenges and risks to children and adults both inside and outside of school, including when they are remote learning online at home. Where children are being asked to learn online at home, the DFE has provided advice to support schools to do so safely.

1.3. All staff should be aware that technology is a significant component in many safeguarding and wellbeing issues. Children are at risk of abuse online as well as face to face. In many cases, abuse will take place concurrently via online channels and in daily life. Children can also abuse other children online. This can take the form of abusive, harassing, and misogynistic messages, the non-consensual sharing of indecent images, especially around chat groups, and the sharing of abusive images and pornography, to those who do not want to receive such content.

1.4. Members of staff with appropriate skills, interest and expertise regarding online safety are encouraged to help support the DSL, and any deputy DSLs as appropriate, for example when developing curriculum approaches or making technical decisions. However, the DSL is acknowledged as having overall responsibility for online safeguarding within the school.

1.5. Radnor House 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 material;
- Contact: being subjected to harmful online interaction with other users;
- Conduct: personal online behaviour that increases the likelihood of, or causes, harm;
- Commerce: being exposed to risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

1.6. New technologies are continually enhancing communication, the sharing of information, learning, social interaction and leisure activities. Current and emerging technologies used in and outside of school include:

- websites;
- email and instant messaging;
- blogs;
- social networking sites;
- chat rooms;
- music/video downloads;
- gaming sites;
- text messaging and picture messaging;
- video calls;
- podcasting;
- online communities via games consoles;
- mobile internet devices such as smart phones and tablets; and
- applications used on mobile and other devices.

1.7. This policy complements the Statement of Acceptable Use for all staff, visitors and pupils, and is implemented to protect the interests and safety of the whole school community. It aims to provide clear guidance on how to minimise risks and how to deal with any infringements.

1.8. While exciting and beneficial, both in and out of the context of education, much IT, particularly online resources, is not consistently policed. All users need to be aware of the range of risks associated with the use of these internet technologies.

1.9. At this school we understand the responsibility to educate our pupils about online safety issues, teaching them the appropriate behaviours and critical thinking skills necessary to enable them to remain both safe and within the law when using the internet and related technologies in and beyond the classroom.

1.10. We also encourage anyone, including a pupil who believes our systems are being misused in any way, to speak out and alert us to such possible misuse.

1.11. There are codes of conduct for authorised and responsible use of our system for both staff and pupils. Please refer to the Acceptable Use (IT) Policy – Pupils, and the Acceptable Use (IT) Policy – Staff and Governors for further information.

2. Roles and Responsibilities

2.1 The Board of Governors of the school is responsible for the approval of this policy and for reviewing its effectiveness. The Board delegates the review of this policy to the Principal, which is carried out annually.

2.2 Under KCSIE 2023, the Board of Governors must ensure that appropriate online filters and appropriate monitoring systems are in place, so that pupils are safeguarded from potentially harmful and inappropriate online material.

2.3 The school identifies and assigns roles and responsibilities to manage filtering and monitoring systems, to review filtering and monitoring at least annually, block harmful and inappropriate content without unreasonably impacting teaching and learning, and have effective monitoring strategies in place that meet our safeguarding needs, including a regular review of the processes to see if more needs to be done;

2.4 The Governors must also ensure that safeguarding training for staff, including online safety training, is integrated and considered as part of the whole school safeguarding approach. They also ensure that the children are taught about safeguarding, including online safety.

2.5 The Principal is responsible for the safety of the members of the school community and this includes responsibility for online safety. This responsibility for online safety has been delegated to the Designated Safeguarding Lead (DSL), who has been appointed as Online Safety Co-ordinator.

2.6 The Designated Safeguarding Lead/Online Safety Co-ordinator takes lead responsibility for safeguarding and child protection, including online safety, liaising with the IT Manager regarding the ongoing monitoring and filtering of the internet in school.

2.7 The Designated Safeguarding Lead is expected to:

- liaise with all staff on matters of safety and safeguarding, including online and digital safety;
- be able to understand the unique risks associated with online safety and be confident that

they have the relevant knowledge and up to date capability required to keep children safe while they are online at school; and

- be able to recognise the additional risks that children with SEND face online, for example from online bullying, grooming and radicalisation, and be confident they have the capability to support SEND children to stay safe online;
- keep up to date on current online safety issues and guidance issued by relevant organisations, including the ISI, the Local Authority, CEOP (Child Exploitation and Online Protection), Childnet International, NSPCC and the Local Authority Safeguarding Children Partnership.

2.8 The Senior Leadership Team is expected to ensure that:

- staff, in particular the Online Safety Co-ordinator, are adequately trained about online safety;
- staff are aware of the school procedures and policies that should be followed in the event of the abuse or suspected breach of online safety in connection to the school.
- there are appropriate and up-to-date policies regarding Online Safety, including a Staff Code of Conduct and an Acceptable Use of IT Policy/Agreement, which covers acceptable use of technology by staff and pupils.

2.9 The Online Safety Co-ordinator is responsible for the day-to-day issues relating to online safety, including monitoring the use of the internet and managing the filtering of inappropriate websites. The Online Safety Co-ordinator has responsibility for ensuring this policy is upheld by all members of the school community.

2.10 The school's technical staff have a key role in maintaining a safe technical infrastructure at the school and in keeping abreast of the rapid succession of technical developments. They are responsible for the security of the school's hardware system, its data and for training the school's teaching and administrative staff in the use of ICT. They routinely use software to monitor the use of the internet for pupils and staff, which produces filtering reports and instant notifications regarding inappropriate usage, and which go direct to the DSL. Emails are not routinely monitored unless a cause for concern has been raised.

2.11 Where pupils are being asked to learn online at home, the DfE has provided advice to support schools to ensure this is done so safely: safeguarding-in-schools-collegesand-other-providers and safeguarding-and- remote-education. For specific details regarding how the school has organised its home learning programme, technology and online security, please refer to the Remote Teaching and Learning Policy.

2.12 All teaching and support staff are required to sign a statement saying that they have read and understood the school's Staff Code of Conduct, which details the mandatory procedures regarding online safety, and the Acceptable Use of IT Policy before accessing the school's systems. As with all issues of safety at school, staff are encouraged to create a talking and listening culture in order to address any online safety issues which may arise in classrooms on a daily basis.

2.13 Pupils are responsible for using the school IT systems in accordance with the school's Acceptable Use of IT Policy for pupils. They have to signal their agreement to it at every login and they have a responsibility to speak out when they believe that the school's systems are being abused in any way.

2.14 The school believes that it is essential for parents to be fully involved with promoting online safety, both in and outside of school. We regularly consult and discuss online safety with parents and seek to promote a wide understanding of the benefits and risks related to internet usage. The school will

always contact parents if it has any concerns about pupils' behaviour in this area and likewise it hopes that parents will feel able to share any concerns with the school. Parents are responsible for endorsing their child's confirmation of adherences to the school's acceptable use of IT.

3 Education and Training

3.1 Staff: Awareness and Training

New teaching staff receive information about online safety and acceptable use of IT as part of their induction, and all teaching staff receive regular updates on online safety issues in the form of targeted training and internal briefings, and are made aware of their individual responsibilities relating to the safeguarding of children within the context of online safety.

All staff working with children are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following school online safety procedures. When children use school computers, staff should make sure children are fully aware of the agreement they are making to follow the school's acceptable use guidelines.

Teaching staff are encouraged to incorporate online safety activities and awareness within their subject areas and through a culture of talking about issues as they arise. They should know what to do in the event of misuse of technology by any member of the school community.

A safeguarding referral form must be completed by staff via CPOMS as soon as possible if any incident relating to online safety occurs and be sent directly to the DSL.

3.2 Pupils: Online Safety in the Curriculum

IT and online resources are used increasingly across the curriculum. We believe it is essential for online safety guidance to be given to pupils on a regular and meaningful basis. We continually look for new opportunities to promote online safety and regularly monitor and assess our pupils' understanding of it.

The school provides opportunities to teach about online safety within a range of curriculum areas and IT lessons. Educating pupils on the dangers of technologies that may be encountered outside school will also be carried out via PSHEE and assemblies, as well as informally when opportunities arise.

At age-appropriate levels, and usually via PSHEE, pupils are taught to look after their own online safety and are taught about recognising online sexual exploitation, stalking and grooming, the risks, and their duty to report any such instances they or their peers come across. Pupils can report concerns to the DSL or to any member of staff at the school.

Pupils are also taught about relevant laws applicable to using the internet, such as data protection and intellectual property, as well as the need to respect other people's information and images.

Pupils should be aware of the impact of cyber-bullying and know how to seek help if they are affected by these issues, as set out in the school's Anti-Bullying Policy. Pupils should approach the DSL or other members of staff, as well as parents and peers, for advice or help if they experience problems when using the internet and related technologies.

3.3 Pupils: Vulnerable Pupils

The school is aware that some pupils are considered to be more vulnerable online due to a range of factors. This may include, but is not limited to, children in care, children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss.

- The school ensures that differentiated and ability-appropriate online safety education, access and support are provided to vulnerable pupils, and it will seek input from specialist staff as appropriate, including the Head of Learning Support.

3.4 Awareness and Engagement with Parents

The school recognises that parents have an essential role to play in enabling children to become safe and responsible users of the internet and associated technologies, and builds a partnership approach to online safety with parents by:

- providing information, guidance and training on online safety in a variety of formats;
- drawing attention to the Online Safety Policy and other online matters via newsletters, letters and the website;
- requiring that parents read online safety information when a pupil joins the school;
- requiring parents to read the school AUP and discuss its implications with their child.

3.5 Reducing Online Risks

The school recognises that the internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace. Therefore, we will:

- regularly review the methods used to identify, assess and minimise online risks;
- examine emerging technologies for educational benefit and undertake appropriate risk assessments before use in school is permitted;
- ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material;

3.6 Filtering and monitoring – The school will ensure that appropriate filtering and monitoring systems are in place when pupils and staff access school systems and internet provision, so that exposure to any risks can be reasonably limited. The UK Safer Internet Centre has published guidance as to what 'appropriate' filtering and monitoring might be: Appropriate Filtering and Monitoring | Safer Internet Centre. We review our approach to this regularly: annually, or more often if circumstances dictate.

3.7 The school uses a wide range of technology in the classroom. All school-owned devices will be used in accordance with the school's Acceptable Use Policy (AUP) and with appropriate safety and security measures in place. Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.

3.8 All members of the school community are made aware of the school's expectations regarding safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos which could cause harm, distress or offence to members of the community. This is clearly outlined in the school's AUP and highlighted through a variety of education and training approaches.

4 Use of School and Personal Devices

4.1 Staff

School devices assigned to a member of staff as part of their role must have a password or device

lock so that unauthorised people cannot access the content. Staff should only use the school device which is allocated to them for school work. When they are not using a device, staff should ensure that it is locked to prevent unauthorised access.

Personal telephone numbers, email addresses or other contact details may not be shared with pupils or parents, and under no circumstances may staff contact a pupil using a personal telephone number, email address, social media or messaging system. Parents should only be connected using recognised channels of communication.

Personal cameras belonging to staff and volunteers are not to be used on the school premises or school grounds at any time. Cameras on staff-owned mobile phones should not be used on school premises or school grounds at any time. No images may be taken of the school or any pupils using mobile phones or personal cameras.

Staff members must at all times act in the best interests of children and young people when creating, participating in or contributing content to social media sites.

Personal mobile phones may be used in dedicated staff areas or in class and teaching rooms only when pupils are not present, or in the event of needing to use the authenticator application.

Staff should not accept mobile phone calls during a lesson or when they are with children. The only exception to this is if the Principal, the Head or a senior member of staff calls a staff member, for example during a sports day or while on a school trip, or if the school office calls in similar circumstances. These calls will only be made in unusual or emergency situations.

Staff are advised to ensure that Bluetooth or other forms of communication, such as 'Airdrop', are hidden or disabled during lesson times.

School cameras may be used for official photographs under the direction of the Principal. These photographs must only be downloaded using the school's computers and not onto a personal, private computer. Please refer to the Staff Code of Conduct for further details.

If a member of staff breaches the school Online Safety Policy, action will be taken in line with the Staff Code of Conduct.

If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or to have committed a criminal offence, the police will be contacted.

4.2 Pupils

If pupils in Years 7-11 bring in mobile phones, e.g. for use during the journey to and from school, they should be kept switched off and stored in their bags or lockers.

The school recognises that mobile devices are sometimes used by pupils for medical purposes or as an adjustment to assist pupils who have disabilities or special educational needs. Where a pupil needs to use a mobile device for such purposes, the pupil's parents should arrange a meeting with the Head of Learning Support to agree how the school can appropriately support such use. The Head of Learning Support will then inform the pupil's teachers and other relevant members of staff about how the pupil will use the device at school.

Pupils in Year 9 and above may bring in school-approved devices and connect to the school Wi- Fi network as part of the school's Bring Your Own Device (BYOD) programme. These devices will

remain the responsibility of the child in case of loss or damage and will be used at the class teacher's discretion during lesson time and within designated study areas.

Where pupils' mobile phones or personal devices are used when learning at home, this will be in accordance with the school Acceptable Use Policy and Remote Teaching and Learning Policy.

Mobile phones and personal devices must not be taken into examinations. Pupils found in possession of a mobile phone or personal device which facilitates communication or internet access during an exam will be reported to the appropriate examining body, which may result in the withdrawal from either that examination or all examinations.

Any concerns regarding pupils' use of mobile technology or policy breaches will be dealt with in accordance with our existing policies, including Anti-Bullying, Safeguarding and Behaviour.

Staff may confiscate a pupil's mobile phone or device if they believe it is being used to contravene our Safeguarding, Behaviour or Anti-Bullying policies.

Searches of mobile phone or personal devices will be carried out in accordance with the DfE, 'Searching, Screening and Confiscation' guidance: Searching, screening and confiscation at school - GOV.UK (www.gov.uk)

Pupils' mobile phones or devices may be searched by a member of staff with the consent of the pupil or a parent. Content may be deleted or requested to be deleted if it contravenes our policies.

Mobile phones and devices that have been confiscated will be held in a secure place and released to parents.

Appropriate sanctions and/or pastoral/welfare support will be implemented in line with our Behaviour Policy.

Concerns regarding policy breaches by pupils will be shared with parents as appropriate.

Where there is a concern that a child is at risk of harm, we will respond in line with our Safeguarding Policy.

If there is suspicion that material on a pupil's personal device or mobile phone may be illegal, or may provide evidence relating to a criminal offence, the device will be handed over to the police for further investigation.

5 Use of Internet and Email

5.1 Staff

Staff must not access social networking sites, personal email, any website or personal email which is unconnected with school work or business from school devices while teaching or in front of pupils. Such access may only be made while in staff-only areas of school.

When accessed from personal devices away from school premises, staff must use social networking sites with extreme caution, being aware of the nature of what is published online and its potential impact on their professional position and the reputation of the school.

The school has taken all reasonable steps to ensure that the school network is safe and secure. Staff should be aware that email communications through the school network and staff email addresses are monitored.

Staff must immediately report to the DSL, who is the Online Safety Co-ordinator, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature, and must not respond to any such communication.

Any online communications must not either knowingly or recklessly:
harm or place a child or young person at risk of harm;

- bring Radnor House into disrepute;
- breach confidentiality;
- breach copyright;
- breach data protection legislation; or do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by:
    - making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age;
    - using social media to bully another individual;
    - liking and/or disliking and/or retweeting (or the equivalent) any post or other element of social media; and
    - posting links or material which is discriminatory or offensive.

Under no circumstances should school pupils or parents be added as social network 'friends'.

Any digital communication between staff and pupils or parents must be professional in tone and content. Under no circumstances may staff contact a pupil or parent using any personal email address. The school ensures that staff have access to their work email address when offsite, for use as necessary on school business.

5.2 Pupils

All pupils are issued with their own school login (personal school email addresses) for use on our network and to facilitate cloud resources. Access is via this personal login, which is password protected. This official email service may be regarded as safe and secure, and must only be used for school work: assignments, research and projects. Pupils should be aware that digital communication is monitored.

There is strong anti-virus and firewall protection on our network, which is regularly reviewed to ensure that the filtering and monitoring are appropriate. Spam emails and certain attachments will be blocked automatically by the email system. If this causes problems for school work, pupils should contact the Online Safety Co-ordinator for assistance.

Pupils should immediately report, to the DSL or another member of staff, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening, violent, sexual or bullying in nature, and must not respond to any such communication.

The school expects pupils to think carefully before they post any information online including liking and/or disliking and/or retweeting (or the equivalent) any post or other element of social media. Content posted should not be able to be deemed inappropriate or offensive, or likely to cause embarrassment to the individual or others.

Pupils must report any accidental access to materials of a violent or sexual nature directly to the DSL

or another member of staff. Deliberate access to any inappropriate materials by a pupil will be dealt with under the school's Behaviour Policy. Pupils should be aware that all internet usage via the school's systems and its Wi-Fi network is monitored.

Certain websites are automatically blocked by the school's filtering system. If this causes problems for school work, pupils should contact the DSL or another member of staff.

6 Social Media

6.1 The term social media may include (but is not limited to): blogs; wikis; social networking sites; forums; bulletin boards; online gaming; apps; video/photo sharing sites; chatrooms and instant messenger.

6.2 Expectations

The expectations regarding positive, safe and responsible use of social media apply to all members of the Radnor House community. The school controls pupil and staff access to social media while using school provided devices and systems on site.

All members of the Radnor House community are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.

Concerns regarding the online conduct of any member of Radnor House community on social media, should be reported to the school and will be managed in accordance with our Anti-Bullying, Behaviour and Safeguarding policies, and the Staff Code of Conduct.

6.3 Staff Personal Use of Social Media

The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.

Staff use of social media forms part of the school's Code of Conduct.

6.4 Pupils' Personal Use of Social Media

Safe and appropriate use of social media is taught to pupils as part of an embedded and progressive education approach, via age appropriate sites and resources.

The school is aware that many popular social media sites state that they are not for children under the age of 13. Therefore, the school will not create accounts specifically for children under this age.

Any concerns regarding pupils' use of social media, both at home and at school, will be dealt with in accordance with existing school policies including Anti-Bullying and Behaviour. Concerns will also be raised with parents as appropriate, particularly regarding underage use of social media sites or tools.

6.5 Official School Use of Social Media

The official use of social media sites by the school only takes place with clear educational or community engagement objectives, with specific intended outcomes.

Official school social media channels have been set up as distinct and dedicated social media sites or

accounts for educational or engagement purposes only. Official social media sites are suitably protected and, where possible, run and/or linked to/from the school website.

Official social media use will be conducted in line with existing policies, including: Anti-Bullying, Data Protection and Safeguarding, and the Staff Code of Conduct.

Any official social media activity involving pupils will be moderated by the school where possible.

The school will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.

6.6 Staff Guidelines

Members of staff who follow and/or 'like' the school social media channels are advised to use dedicated (i.e. not personal) accounts, where possible, to avoid blurring professional boundaries.

If members of staff are participating in online social media activity as part of their capacity as an employee of the school, they will:

- be professional, responsible, credible and fair at all times and aware that they are an ambassador for the school;
- disclose their official role and/or position, but make it clear that they do not necessarily speak on behalf of the school;
- ensure that they have appropriate written consent before posting images on the official social media channel;
- not disclose information, make commitments or engage in activities on behalf of the school unless they are authorised to do so;
- not engage with any direct or private messaging with current, or past, pupils and parents;
- immediately inform their line manager, the Designated Safeguarding Lead and/or the Principal of any concerns, such as criticism, inappropriate content or contact from pupils.

7 Data Storage and Processing

7.1 The school takes its compliance with the General Data Protection Regulation 2018 and the Data Protection Act 2018 seriously. Please refer to the school's Data Protection Policy and the Acceptable Use of IT Policy for further details.

7.2 Staff devices should be encrypted if any data or passwords are stored on them. The school expects all removable media (USB memory sticks, CDs, portable drives) taken outside school or sent by post or courier to be encrypted before sending.

7.3 Staff may only take information offsite when authorised to do so, and only when it is necessary and required in order to fulfil their role. No personal data of staff or pupils should be stored on personal memory sticks, but instead stored on an encrypted USB memory stick provided by school.

7.4 Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of IT must be immediately reported to the Online Safety Co-ordinator.

8 Security and Management of Information Systems

8.1 The school takes appropriate steps to ensure the security of our information systems. This is reviewed annually, or more regularly if circumstances dictate. For further details, please see Appendix 2.

8.2 Staff devices should be encrypted if any data or passwords are stored on them. The school expects all removable media (USB memory sticks, CDs, portable drives) taken outside school or sent by post or courier to be encrypted before sending.

Staff may only take information offsite when authorised to do so, and only when it is necessary and required in order to fulfil their role. No personal data of staff or pupils should be stored on personal memory sticks or personal cloud storage, but instead stored on an encrypted USB memory stick or school provided cloud storage.

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of IT must be immediately reported to the IT team.

8.3 Password Security

Pupils and staff have individual school network logins [email addresses] and storage folders on the server. Staff and pupils are regularly reminded of the need for password security. All pupils and members of staff should:

- use a strong password (usually containing eight characters or more, and containing upper and lower case letters as well as numbers) which, in line with the Cyber Essentials Guidance (a government accredited scheme) should be changed annually by both staff and pupils;
- not write passwords down; and
- not share passwords with pupils or other staff.
-

When accessing MS365 and iSAMS from any location other than the school network, 2-factor authentication protocols will be enforced when accessing the Radnor House Twickenham school systems.

9 Safe Use of Digital and Video Images

9.1 The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying, stalking or grooming to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

9.2 When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet, for example on social networking sites.

9.3 For parents of older children: they 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 on blogs or social networking sites without the permission of the people identifiable in them or (if minors) without the permission of their parents, nor should parents comment on any activities involving other children or pupils in the digital or video images.

9.4 Staff and volunteers are allowed to take digital and video images to support educational aims, but must follow this policy concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment: personal equipment should not be used for such purposes.

9.5 Care should be taken when taking digital and video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

9.6 Pupils must not take, use, share, publish or distribute images of others without their permission.

9.7 Photographs published on the school website, or displayed elsewhere, that include pupils, will be selected carefully and will comply with good practice guidance on the use of such images. Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

9.8 Teachers can use video for live or recorded remote teaching. Please refer to the school's Remote Teaching and Learning Policy for full details and the expectations on its use.

9.9 For safeguarding considerations, teachers can ensure that recorded lessons are uploaded to Stream because it requires a login/password by teachers/pupils to access. Content for parents to access is uploaded to YouTube but with a non-searchable URL so it can only be accessed by a link provided by the school.

9.10 Radnor House recognises that consensual and non-consensual sharing of nude and semi-nude images and/or videos (also known as youth produced/involved sexual imagery or 'sexting') can be a safeguarding issue; all concerns will be reported to and dealt with by the DSL (or deputy). The term 'sharing nudes and semi-nudes' is used to mean the sending or posting of nude or semi-nude images, videos or live streams of/by young people under the age of 18. Creating and sharing nudes and semi-nudes of under-18s (including those created and shared with consent) is illegal which makes responding to incidents complex.

10 Management of Applications which Record Children's Progress (Data and Images)

10.1 The school uses iSAMS to track pupils' progress and share appropriate information with parents. The Principal is ultimately responsible for the security of any data or images held of children. As such, they will ensure that tracking systems are appropriately risk assessed prior to use, and that they are used in accordance with GDPR and data protection legislation. The school's Data Protection Policy and Notices are available on the school website.

To safeguard data:

- only school issued devices will be used for apps that record and store children's personal details, attainment or photographs;
- personal staff mobile phones or devices will not be used to access or upload content;
- school devices will be appropriately encrypted if taken off site to reduce the risk of a data security breach in the event of loss or theft;
- all users will be advised regarding safety measures, such as using strong passwords and logging out of systems;
- parents will be informed of the expectations regarding safe and appropriate use ,prior to being given access; for example, not sharing passwords or images.

11 Radicalisation and the Use of Social Media

11.1 The internet, and the use of social media in particular, has become a major way to communicate with others, especially young people, which has provided access for like-minded people to create an online community and confirm extreme beliefs such as ideological views or the use of violence to solve problems.

11.2 In line with the Prevent guidance (updated December 2023), protecting children from the risk of

radicalisation, the school has a number of measures in place to ensure that children are safe from terrorist and extremist material when accessing the internet in school, and to help prevent the use of social media for this purpose:

- website filtering is in place to help prevent access to terrorist and extremist material and social networking sites such as Facebook, Instagram or X by pupils;
- pupils, parents and staff are educated in safe use of social media and the risks posed by online activity, including from extremist and terrorist groups.

11.3 Further details on how social media is used to promote extremism and radicalisation can be found on the Educate Against Hate site, which is designed to equip schools and college leaders, teachers and parents with the information, tools and resources they need to recognise and address extremism and radicalisation in young people, including in online issues. Educate Against Hate - Prevent Radicalisation & Extremism

12 Responding to Online Safety Incidents and Concerns

12.1 All members of the school community are made aware of the reporting procedure for online safety and safeguarding concerns regarding pupil welfare, including: breaches of filtering, youth produced sexual imagery (sexting), upskirting, cyberbullying, sexual harassment and illegal content. The school requires staff, parents and pupils to work in partnership to resolve online safety issues.

12.2 All members of the school community must respect confidentiality and the need to follow the official school procedures for reporting concerns. For further detailed information, the school Safeguarding Policy, Complaints Policy and Procedures and Whistleblowing Policy can be found on the school website.

12.3 After any investigations are completed, the school will debrief, identify lessons learnt and implement any policy or curriculum changes as required.

12.4 If the school is unsure how to proceed with an incident or concern, the DSL will seek advice from the Local Education Safeguarding Team. Where there is suspicion that illegal activity has taken place, the school will contact the Education Safeguarding Team or the police.

12.5 Any allegations regarding a member of staff's online conduct will be referred to the Principal and discussed with the DSL and the LADO if necessary. Appropriate action will be taken in accordance with the Staff Code of Conduct.

12.6 When made aware of concerns involving consensual and non-consensual sharing of nudes and semi-nude images and/or videos by children, staff are advised to:

- report any concerns to the DSL immediately;
- never view, copy, print, share, store or save the imagery, or ask a child to share or download it – this may be illegal. If staff have already viewed the imagery by accident, this must immediately be reported to the DSL;
- not delete the imagery or ask the child to delete it;
- not say or do anything to blame or shame any children involved;
- explain to child(ren) involved that they will report the issue to the DSL and reassure them that they will receive appropriate support and help;
- not ask the child or children involved in the incident to disclose information regarding the imagery and not share information about the incident with other members of staff, the child(ren) involved or their, or other, parents and/or carers. This is the responsibility of the DSL.

The DSL will respond to the concerns as set out in the non-statutory UKCIS guidance: Sharing nudes and semi-nudes: advice for education settings working with children and young people - GOV.UK (www.gov.uk)

12.7 For further details regarding the procedures for responding to specific online incidents or concerns, please contact the school Online Safety Lead.

13 Visitors' Use of Mobile and Smart Technology

13.1 Visitors, including volunteers and contractors who are on site for regular or extended periods of time, are expected to use mobile and smart technology in accordance with our Acceptable Use of Technology Policy and other associated policies, including child protection.

13.2 Visitors' Wi-Fi codes are available from Reception.

13.3 If visitors require access to mobile and smart technology, for example when working with pupils as part of multi-agency activity, this will be discussed with the IT Services Manager prior to use being permitted and will be noted on the visitor risk assessment form held by HR.

13.4 Members of staff are expected to challenge visitors if they have concerns about their use of mobile and smart technology and will inform the DSL or IT Manager of any breaches of our policy.

14 Misuse

14.1 The school will not tolerate illegal activities or activities that are inappropriate in a school context. The school will always report illegal material and illegal activity to the police and/or the Local Children Safeguarding Partnership. If the school discovers that a child or young person is at risk as a consequence of online activity, it may seek assistance from the local children's services and/or police.

14.2 Incidents of misuse or suspected misuse must be investigated by staff and, where appropriate, this will be in accordance with the school's Safeguarding Policy and related procedures and/or the Anti-Bullying Policy.

14.3 The school will impose a range of sanctions on any pupil who misuses technology to bully, harass or abuse another pupil in line with our Anti-Bullying Policy, noting that instances of bullying may be child protection concerns.

15 Complaints

15.1 As with all issues of safety at the school, if a member of staff, a pupil or a parent has a complaint or concern relating to online safety, prompt action will be taken to deal with it. Complaints should be addressed to the DSL in the first instance, who will undertake an immediate investigation and liaise with the Senior Leadership Team and any members of staff or pupils involved. Please see the Complaints Procedures for further information.

15.2 Incidents of, or concerns around, online safety will be recorded and reported to the school's Designated Safeguarding Lead.

Appendix 1 – Online Safety (KCSIE 2023)

It is essential that children are safeguarded from potentially harmful and inappropriate online material. An effective whole school approach to online safety empowers a school to protect and educate pupils and staff in their use of technology and establishes mechanisms to identify, intervene in and escalate any concerns where appropriate.

The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:

- **content:** being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
- **contact:** being subjected to harmful online interaction with other users; for example: 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; for example, 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. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

Schools and colleges should ensure online safety is a running and interrelated theme whilst devising and implementing policies and procedures. This will include considering how online safety is reflected as required in all relevant policies and considering online safety whilst planning the curriculum, any teacher training, the role and responsibilities of the designated safeguarding lead and any parental engagement.

Online Safety Policy

Online safety and the school or college's approach to it should be reflected in the child protection policy.

Considering the 4Cs (above) will provide the basis of an effective online policy. The school or college should have a clear policy on the use of mobile and smart technology. Amongst other things this will reflect the fact many children have unlimited and unrestricted access to the internet via mobile phone networks (i.e. 3G, 4G and 5G). This access means some children, whilst at school or college, sexually harass their peers via their mobile and smart technology, share indecent images: consensually and non-consensually (often via large chat groups), and view and share pornography and other harmful content. Schools and colleges should carefully consider how this is managed on their premises and reflect in their mobile and smart technology policy and their child protection policy.

Remote Learning

Where children are being asked to learn online at home the Department has provided advice to support schools and colleges do so safely: safeguarding and remote education. The NSPCC and LGFL also provide helpful advice:

- NSPCC Learning - Undertaking remote teaching safely during school closures
- The National Grid for Learning - Safe Remote Learning (lgfl.net)

Filters and Monitoring

While considering their responsibility to safeguard and promote the welfare of children and provide them with a safe environment in which to learn, governing bodies and proprietors should be doing all that they reasonably can to limit children's exposure to the above risks from the school's or college's IT system. As part of this process, governing bodies and proprietors should ensure their school or college has appropriate filters and monitoring systems in place. Governing bodies and proprietors should consider the age range of their children, the number of children, how often they access the IT system and the proportionality of costs vs risks.

The appropriateness of any filters and monitoring systems are a matter for individual schools and colleges and will be informed in part, by the risk assessment required by the Prevent Duty. The UK Safer Internet Centre has published guidance as to what "appropriate" filtering and monitoring might look like: Appropriate Filtering and Monitoring | Safer Internet Centre.

Support for schools when considering what to buy and how to buy it is available via the: schools' buying strategy with specific advice on procurement here: Buying for schools - Guidance - GOV.UK (www.gov.uk).

Information Security and Access Management

Education settings are directly responsible for ensuring they have the appropriate level of security protection procedures in place, in order to safeguard their systems, staff and learners and review the effectiveness of these procedures periodically to keep up with evolving cyber-crime technologies. Guidance on e-security is available from the National Education Network The National Grid for Learning - Safe Remote Learning (lgfl.net) NEN. In addition, broader guidance on cyber security including considerations for governors and trustees can be found at NCSC.GOV.UK.

Reviewing Online Safety

Technology, and risks and harms related to it evolve and changes rapidly. Schools and colleges should consider carrying out an annual review of their approach to online safety, supported by an annual risk assessment that considers and reflects the risks their children face. A free online safety self-review tool for schools can be found via the 360 safe website.

UKCIS has published Online safety in schools and colleges: Questions from the governing board. The questions can be used to gain a basic understanding of the current approach to keeping hildren safe online; learn how to improve this approach where appropriate; and find out about tools which can be used to improve the approach. It has also published an Online Safety Audit Tool which helps mentors of trainee teachers and newly qualified teachers induct mentees and provide ongoing support, development and monitoring.

When reviewing online safety provision, the UKCIS external visitors guidance highlights a range of resources which can support educational settings to develop a whole school approach towards online safety.

Appendix 2 – Security and Management of Information Systems

The school takes appropriate steps to ensure the security of our information systems including, but not limited to:

- virus protection being updated regularly;
- encryption for personal data sent over the Internet or taken off site (such as via portable media storage) or access via appropriate secure remote access systems;
- not using portable media without specific permission; portable media will be checked by an anti-virus /malware scan before use;
- not downloading unapproved software to work devices or opening unfamiliar email attachments;
- regularly checking files held on the school's network;
- the appropriate use of user logins and passwords to access the school network;
- specific user logins and passwords will be enforced for all but the youngest users;
- all users are expected to log off or lock their screens/devices if systems are unattended.

Appendix 3 – Sources of Information for Schools and Parents to Keep Children Safe Online (KCSIE 2023)

There is a wealth of information available to support schools, colleges and parents/carers to keep children safe online. The following list is not exhaustive but should provide a useful starting point:

Advice for Governing Bodies/Proprietors and Senior Leaders

- Childnet provide guidance for schools on cyberbullying
- Educateagainsthate provides practical advice and support on protecting children from extremism and radicalisation
- London Grid for Learning provides advice on all aspects of a school or college's online safety arrangements
- NSPCC provides advice on all aspects of a school or college's online safety arrangements
- Safer recruitment consortium "guidance for safe working practice", which may help ensure staff behaviour policies are robust and effective
- Searching screening and confiscation is departmental advice for schools on searching children and confiscating items such as mobile phones
- South West Grid for Learning provides advice on all aspects of a school or college's online safety arrangements
- Use of social media for online radicalisation - A briefing note for schools on how social media is used to encourage travel to Syria and Iraq
- UK Council for Internet Safety have provided advice on, and an Online Safety Audit Tool to help mentors of trainee teachers and newly qualified teachers induct mentees and provide ongoing support, development and monitoring
- Department for Digital, Culture, Media & Sport (DCMS) Online safety guidance if you own or manage an online platform provides practical steps on how companies can embed safety into the design of their online platforms. It offers information on common platform features and functions (such as private messaging) and their risks, as well as steps that can be taken to manage that risk.
- Department for Digital, Culture, Media & Sport (DCMS) A business guide for protecting children on your online platform provides guidance to businesses on how to protect children on their online platform. It outlines existing regulatory requirements and provides best practice advice on how to protect children's personal data, ensure content is appropriate for the age of users, ensure positive user-to-user interactions and address child sexual exploitation and abuse.

Remote Education, Virtual Lessons and Live Streaming

- Case studies on remote education practice are available for schools to learn from each other
- Departmental guidance on safeguarding and remote education including planning remote education strategies and teaching remotely
- London Grid for Learning guidance, including platform specific advice
- National cyber security centre guidance on choosing, configuring and deploying video conferencing
- National cyber security centre guidance on how to set up and use video conferencing
- UK Safer Internet Centre guidance on safe remote learning

Support for Children

- Childline for free and confidential advice
- UK Safer Internet Centre to report and remove harmful online content
- CEOP for advice on making a report about online abuse

Parental Support

- Childnet offers a toolkit to support parents and carers of children of any age to start discussions about their online life, to set boundaries around online behaviour and technology use, and to find out where to get more help and support
- Commonsensemedia provide independent reviews, age ratings, & other information about all types of media for children and their parents

- Government advice about protecting children from specific online harms such as child sexual abuse, sexting, and cyberbullying
- Government advice about security and privacy settings, blocking unsuitable content, and parental controls
- Internet Matters provide age-specific online safety checklists, guides on how to set parental controls on a range of devices, and a host of practical tips to help children get the most out of their digital world
- Let's Talk About It provides advice for parents and carers to keep children safe from online radicalisation
- London Grid for Learning provides support for parents and carers to keep their children safe online, including tips to keep primary aged children safe online
- Stopitnow resource from The Lucy Faithfull Foundation can be used by parents and carers who are concerned about someone's behaviour, including children who may be displaying concerning sexual behaviour (not just about online)
- National Crime Agency/CEOP Thinkuknow provides support for parents and carers to keep their children safe online
- Net-aware provides support for parents and carers from the NSPCC and O2, including a guide to social networks, apps and games
- Parentzone provides help for parents and carers on how to keep their children safe online
- Parent info from Parentzone and the National Crime Agency provides support and guidance for parents from leading experts and organisations
- UK Safer Internet Centre provide tips, advice, guides and other resources to help keep children safe online