PARAYHOUSE SCHOOL
LANGUAGE AND LEARNING FOR LIFE

E-Safety Policy

September 2020

Policy available to parents: on website/request

Policy to be reviewed: Sept 2021

Background / Rationale

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote student achievement. However, the use of these new technologies can put young people at risk within and outside the school and has become a key component of many safeguarding issues. Given the specific challenges that our students face with communication and social interaction, the school has an increased responsibility to ensuring that they can access their technologies in an appropriate and safe manner including those that use AAC devices.

Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Un-authorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- Child Sexual Exploitation
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- The potential for excessive use, which may impact on the social and emotional development and learning of the young person
- Radicalisation

Many of these risks reflect situations in the off-line world, and it is essential that this e-safety policy is used in conjunction with other school policies (e.g. behaviour, anti-bullying and child protection policies).

The breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk:
• **content:** being exposed to illegal, inappropriate or harmful material; for example pornography, fake news, racist or radical and extremist views;
• **contact:** being subjected to harmful online interaction with other users; for example commercial advertising as well as adults posing as children or young adults; and

• **conduct:** personal online behaviour that increases the likelihood of, or causes, harm; for example making, sending and receiving explicit images, or online bullying.

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision, to build students' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks. An effective approach to online safety empowers a school to protect and educate the whole school community in their use of technology and establishes mechanisms to identify, intervene in, and escalate any incident where appropriate.

Development and Monitoring

Persons Responsible:
Accessing Technology Co-ordinator: Holly Bristow (Headteacher)
Designated Safeguarding Lead: Verity Carnevale (Headteacher)

This e-safety policy has been developed by the Accessing Technology Co-ordinator and the Designated Safeguarding Lead in conjunction with the School Leadership team. As part of this policy, records will be maintained of e-safety related incidents involving staff and students and any incidents recorded will be treated in accordance with our safeguarding procedures. This policy will be reviewed at least annually.

The school will monitor the impact of the policy using:
• Feedback from staff, students, parents / carers, governors
• Logs of reported incidents

Scope of the Policy

This policy applies to all members of the school community (including staff, students, volunteers, parents / carers, visitors) who have access to and are users of school ICT systems, both in and out of school.

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other on-line e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

The 2011 Education Act increased these powers with regard to the search for and of electronic devices and the deletion of data. In the case of both these acts, action can only be taken in relation to our published Behaviour Policy. The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

Roles and Responsibilities

Governors:
Governors are responsible for the approval of the e-safety policy and for reviewing the effectiveness of the policy.

Headteacher / Senior Leaders:
- The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community, though the day-to-day responsibility for e-safety will be delegated to the Accessing Technology Co-ordinator/Designated Safeguarding Lead.
- The Headteacher is responsible for the implementation and effectiveness of this policy. She is also responsible for reporting to the Governing Body on the effectiveness of the policy and, if necessary, make any necessary recommendations re further improvement.
- The Headteacher / Senior Leaders are responsible for ensuring that the Accessing Technology Coordinator/ Designated Safeguarding Lead and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles.
- The Headteacher / Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Headteacher, DSL and another member of the Senior Leadership should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. (See Managing Allegations against a member of staff policy/guidance)

Accessing Technology Co-ordinator + Designated Safeguarding Lead
- Take day-to-day responsibility for e-safety issues and have a leading role in establishing and reviewing the school e-safety policies / documents
- Ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place
- Report to the School Leadership Team serious breaches of the e-safety policies
- Provide training and advice for staff

- Receive reports of e-safety incidents and create a log of incidents to inform future e-safety developments
- Should be trained in e-safety issues and be aware of the potential for serious child protection issues to arise from: • Sharing of personal data • Access to illegal / inappropriate materials • Inappropriate on-line contact with adults / strangers • Potential or actual incidents of grooming • Cyber-bullying • Sexting • Revenge pornography • Radicalisation (extreme views) • CSE

Teaching and Support Staff

All staff are required to read and sign an Acceptable Use of Technology Agreement which clearly states the responsibilities of staff using technology in the work place. This will be signed when they commence their employment at Parayhouse School and will be re-enforced each year during the staff's e-safety session. All staff will attend both training on e-safety and Prevent (dealing with radicalisation & extremism).

The AUP list the responsibilities of all staff and covers the use of digital technologies in school: i.e. E-mail, Internet, Intranet and network resources, software, equipment and systems and complements the General Teaching Council's Code of Practice for Registered Teachers:

- have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- read, understand and sign the e–safety policy and School Staff Acceptable Use Agreement (AUP)
- Report any suspected misuse or problem to the Designated Safeguarding Lead for investigation / action / sanction
- Maintain professional conduct in digital communications with Students and parents / carers (email / voice)
- Support students to understand and follow, as appropriate for age and ability, the school e-safety and acceptable use policy
- Ensure students understand and follow e-safety rules, and they know that if these are not adhered to, sanctions will be implemented in line with our behaviour and anti bullying policies.
- Ensure that in lessons where internet use is planned students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Students:

- Are responsible for using the school ICT systems in accordance with the Student Acceptable Use Policy, which they will be expected to agree to before being given access to school systems, where appropriate for age and ability.

- With support, should understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so (where appropriate for age and ability)
- Will be expected to follow school rules relating to this policy e.g. safe use of cameras, cyberbullying etc.
- With support, should understand that the school's e-safety policy covers their actions out of school, if related to their membership of the school, (where appropriate for age and ability).

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through parents' evenings, letters, website / e-safety campaigns / literature. Parents and carers will be responsible for:
- Endorsing (by signature) the Student / Student Acceptable Use Policy
- Accessing the school website / on-line Student records in accordance with the relevant school Acceptable Use Policy.
- Parents / carers should understand that school has a duty of care to all Students. The misuse of nonschool provided systems, out of hours, will be investigated by the school in line with our behaviour, anti-bullying and safeguarding policies.

Education

Students
Students' e-safety education will be provided in the following ways, as appropriate to their age and ability:
• A planned e-safety programme should be provided as part of Accessing Technology/ PHSE / other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school.
• Key e-safety messages should be reinforced as part of assemblies and tutorial / pastoral activities where possible
• Students should be encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
• Where possible, students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
• Students are taught the importance of keeping information such as their password safe and secure.
• Rules for the use of ICT systems / internet will be made available for students to read

• Staff should act as good role models in their use of ICT, the internet and mobile devices

Parents

As a school we believe it is our duty to support parent and carers in keeping their child safe while using technology within the home environment. Computers and other devices in the home are more open and don't have the security features that we have in school, which does make the child more vulnerable in this environment. Our designated family support manager makes home visits to all students and will discuss the responsible use of the internet at home with their parents and carers. The school web site will have information regarding e-safety for parents / carers and young people.

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. The school will therefore seek to provide information and awareness to parents and carers through: • Letters, web site • Parents evenings • Reference to external e-safety websites • Family learning opportunities

Staff

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

• A programme of e-safety training will be made available to staff alongside wider Safeguarding Training. An audit of the e-safety training needs of all staff will be carried out regularly.

• All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand and agree to adhere to the school e-safety policy and Acceptable Use Policies

• The DSL and Accessing Technology Co-ordinator will provide advice / guidance / training to individuals as required

Technical – Infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

• School ICT systems will be managed through the managed service provider, in ways that ensure that the school meets the e-safety technical requirements for the DfE
• Servers, wireless systems and cabling must be securely located and physical access restricted
• All users will have clearly defined access rights to school ICT systems
• Staff will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security
• The school maintains and supports the managed filtering service provided by LGFL. Any incidents or activities regarding filtering will be handled in accordance with the school policy.
• Remote management tools are used by the managed service provider to manage workstations.
• Appropriate security measures are in place, provided by the managed service provider, to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data
• Guest access to the school network will be authorised by the School Office Team through the provision of limited access guest accounts, which do not give access to personal information about Students or staff.
• The school infrastructure and individual workstations are protected by up to date anti-virus software
• Personal data should not be sent over the internet or taken off the school site unless safely encrypted or otherwise secured in accordance with the school GDPR Policy

The Curriculum

• E-safety should be a focus in all areas of the curriculum, and staff should reinforce e-safety messages in the use of ICT across the curriculum.
• Good e-safety practice is an integral part of the school Accessing Technology curriculum and will be taught to students as part of their learning.
• Where students are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.

Use of digital photographs and video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff and students need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on

the internet forever and may cause harm or embarrassment to individuals in the short or longer term.
The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:
• Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the storing, sharing, distribution and publication of those images. Those images should only be taken on school equipment. The personal equipment of staff should not be used for such purposes.
• Care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
• Students must not take, use, share, publish or distribute images of others without their permission
• Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.
• Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.
• Written permission from parents or carers will be obtained before photographs of students are published on the school website

Data Protection
Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018. More detailed guidance on the collection, handling and storage of personal data can be found in the school GDPR Policy.

Communications
When using communication technologies the school considers the following as good practice:
• The official school email service may be regarded as safe and secure. Students should therefore not use other email systems when in school, or on school systems.
• Users need to be aware that email communications may be monitored.
• Users must immediately report, to the E-Safety Coordinator – in accordance with the school policy - the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
• Any digital communication between staff and students or parents / carers must be professional in tone and content and be via official used systems.
• Individual official school email addresses are provided to parents for specific issues related to learning or the school day, however parents are encouraged to

send most correspondence (particularly that related to absence or medical issues) through the school office.

- Staff personal mobile phone numbers should not be shared with students or parents
- Students should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be placed on the school website and only official school emails should be identified within it.
- The school allows staff to bring in their own personal devices, including mobile phones, for their own use. Under no circumstance should these be used to take photos of students or to communicate with parents.

Responding to incidents of misuse

There may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse by students, staff or any other user appears to involve illegal activity, then the response to the incident should be following in accordance with the safeguarding policy and if necessary, the police should also be informed. Illegal activity include:

- Child sexual abuse images
- Adult material, which potentially breaches the Obscene Publications Act
- Criminally racist material
- Other criminal conduct, activity or materials

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner.

Please refer to the school's Child Protection and Safeguarding Policy for further information on responding to and reporting incidences of Sexting.

Safety and Responsibility for Students

Although some of our students are unable to access the internet we have a good percentage of students who are able to use the internet independently and therefore are at risk from either deliberately accessing inappropriate material or, due to their level of literacy, accidently accessing harmful sites.

No child is able to access the internet in school without their parents giving permission to do so. This consent form is filled in when the child starts school and is kept on record until they leave; it will only need amending if a parent/carer would like to change it.

All children are supervised in school whilst using the internet and all are made aware that all their activity within school is monitored.

All Students will receive e-safety training in Accessing Technology lessons. All students will be taught how to use all technologies in a responsible and safe way.

Home Learning

As a result of the coronavirus (COVID-19) outbreak, students may need to access remote learning provided by the school, which may include online contact. Remote education is a new experience for both staff and pupils, so it's important that schools understand how to approach safeguarding procedures online. Staff should follow the principles set out in the school's Safeguarding Policy, Acceptable Use of Technology agreement and Code of Conduct when providing home learning support.

Communication with parents

The school will ensure that all online learning is at the consent of parents and they are kept informed as to the nature of this learning.
It's especially important for parents and carers to be aware of what their children are being asked to do online, including:

- sites they will be asked to use
- school staff their child will interact with

The school is committed to ensuring a safe online environment and will encourage parents and carers to set age-appropriate parental controls on digital devices and use internet filters to block malicious websites.

Reporting Concerns

It is essential to have and communicate clear reporting routes so that children, teachers, parents and carers can raise any safeguarding concerns.
Staff are expected to use the school's online reporting system My Concern in line with our Safeguarding policy and parents are provided contacts for all key personnel in the event that they wish to report or discuss any concerns.

Virtual Learning

Where education may have to take place remotely, it's important for schools, teachers and pupils to maintain professional practice as much as possible. When communicating online with parents and pupils, staff should:

- communicate within school hours as much as possible (or hours agreed with the school to suit the needs of staff)
- communicate through the school channels approved by the senior leadership team
- use school email accounts (not personal ones)
- use school devices over personal devices wherever possible
- not share personal information

The agreed school platform for virtual learning is Zoom. The school will provide advice and regulations to parents on the use of this system.

All staff and students using this platform will be advised to:

- Use a quiet space
- To ensure the background has no sensitive or personal information visible
- All calls will take place with 2 adults present, and parents will be advised to accompany their child on all calls.

.

Personal data and GDPR

The school will continue to follow the guidance outlined in the data protection: toolkit for schools when managing personal data and will consider:

- taking care not to share contact details when emailing multiple people
- being careful when sharing usernames and other personal data for access to online resources
- providing access to school data systems safely

The school will only use systems suitable for our students' age and development and only with the support of adults. We will seek parental consent for all online lessons.

Staff will use parents' or carers' email addresses or phone numbers to communicate with children only using school accounts

All calls must take place from a blocked number so teacher's personal contact details are not visible.

If staff members are accessing families' contact details at home, they must comply with the Data Protection Act 2018.

Parayhouse School
Acceptable Use of Technology Code of Conduct

Introduction

ICT in its many forms – internet, email, mobile devices etc – are now part of our daily lives. It is our duty to ensure that they are used safely and responsibly. All staff at Parayhouse School are aware of the following responsibilities:

• All Staff, Governors and visitors understand that ICT includes a wide range of systems, including mobile phones, digital cameras, laptops and tablets.

• All staff, Governors and visitors understand that it is a disciplinary offence to use the school's ICT equipment for any purpose not permitted by its owner.

• No staff, Governors or visitors will disclose any passwords provided to them by the school.

• All staff, Governors and visitors understand that they are responsible for all activity carried out under their username.

• All staff, Governors and visitors understand that their use of the internet may be monitored and if anything untoward is uncovered, could be logged and used in line with any disciplinary procedures. If an e-safety incident should occur, staff will report it to the Senior or Deputy Designated Professional for Safeguarding as soon as possible.

• All staff, Governors and visitors will only use the school's email / internet / intranet etc and any related technologies for uses permitted by the Head or Governing Body. If anyone is unsure about an intended use, they should speak to the SenLT (senior leadership team) beforehand.

• All staff, Governors and visitors will ensure that data is kept secure and is used appropriately as authorised by the Head or Governing Body

• Personal devices must only be used in the context of school business. Photographs of students must never be saved or stored on personal devices.

• All staff, Governors and visitors using school equipment will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.

• All staff, Governors and visitors will only use the approved email system for school business.

• Images will only be taken, stored and used for purposes within school unless there is parental permission for alternative use. At the start of each year, our parents are asked to sign if they agree to their children's images being used in

our publications or in the local press. If a parent does not agree to this, we ensure that their child's photograph is not used.

• All staff, Governors and visitors will report any incidents of concern regarding staff use of technology and/or children's safety to the Head or the Deputy Designated Professional in line with our school's Safeguarding Policy.

I acknowledge that I have received a copy of the Acceptable Use Code of Conduct

Full Name _____

Signature _____

Date _____

ELECTRONIC DEVICES

We appreciate that these are part of everyday life for many of our students, and also that students travelling long distances rely on them to pass the time. HOWEVER, students must respect the rules for usage at all times as follows:

- Music listened to on transport should be appropriate with no unsuitable language
- All devices (phones, MP3 players, tablets etc.) should be handed in to staff on arrival
- Students may collect their devices at the end of the day
- Students must not under any circumstances use their devices to take pictures or videos of staff or students including on transport

Any student found to be breaking the above rules will no longer be allowed to bring their device to school.

- Students must not under any circumstances contact fellow students in an inappropriate manner using their devices (including on social media)
- Students must not under any circumstances use their devices (including on social media) to contact a member of staff

Any incident of a student found to be breaking the above rules will be managed in line with the school's behaviour and e-safety policies

Parayhouse accepts no responsibility for these items whilst at school

A range of support sites can be found in Annex C of KCSIE 2020 here: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/912592/Keeping_children_safe_in_education_Sep_2020.pdf

An effective approach to online safety empowers a school or college to protect and educate the whole school or college community in their use of technology and establishes mechanisms to identify, intervene in, and escalate any incident where appropriate.

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

1. content: being exposed to illegal, inappropriate or harmful material; for example pornography, fake news, racist or radical and extremist views;
2. contact: being subjected to harmful online interaction with other users; for example commercial advertising as well as adults posing as children or young adults; and
3. conduct: personal online behaviour that increases the likelihood of, or causes, harm; for example making, sending and receiving explicit images, or online bullying.

Education Opportunities to teach safeguarding, including online safety, are discussed at paragraph 88-90. Resources that could support schools and colleges include:

- "Be Internet Legends" developed by Parent Zone and Google is a free internet safety curriculum with PSHE accredited lesson plans and teaching resources for Key Stage 2 pupils
- "Disrespectnobody" is Home Office advice and includes resources on healthy relationships, including sexting and pornography
- The "Education for a connected world framework" from the UK Council for Internet Safety supports the development of the curriculum and is of particular relevance to RSHE education and Computing. It is designed, however, to be usable across the curriculum and beyond (covering early years through to age 18) and to be central to a whole school or college approach to safeguarding and online safety.
- The PSHE association provides guidance to schools on developing their PSHE curriculum
- "Teaching online safety in school" is departmental guidance outlining how schools can ensure their pupils understand how to stay safe and behave online as part of existing curriculum requirements

- "Thinkuknow" is the National Crime Agency/CEOPs education programme with age specific resources
- The "UK Safer Internet Centre" developed guidance and resources that can help with the teaching of the online safety component of the Computing Curriculum.

Protecting children, 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.

Whilst 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 consider the age range of their pupils, the number of pupils, 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: UK Safer Internet Centre: appropriate filtering and monitoring.

Guidance on e-security is available from the National Education Network. Support for schools is available via the: schools' buying strategy with specific advice on procurement here: buying for schools.

Whilst filtering and monitoring is an important part of the online safety picture for schools and colleges to consider, it is only one part. Governors and proprietors should consider a whole school or college approach to online safety. This will include a clear policy on the use of mobile technology in the school or college. Many children have unlimited and unrestricted access to the internet via 3G, 4G and 5G in particular and the school and college should carefully consider how this is managed on their premises.

119 The Prevent duty Departmental advice for schools and childcare providers and Prevent Duty Guidance For Further Education Institutions

Whilst it is essential that governing bodies and proprietors ensure that appropriate filters and monitoring systems are in place, they should be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regard to online teaching and safeguarding.

Reviewing online safety Technology in this area evolves and changes rapidly. 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 for the governing board to help responsible bodies assure themselves that their online safety arraignments are effective.

Education at home where children are being asked to learn online at home the department has provided advice to support schools and colleges do so safely: safeguarding-in-schools-colleges and-other-providers and safeguarding-and-remote-education Staff training *how does this connect?*

Governors and proprietors should ensure that, as part of the requirement for staff to undergo regularly updated safeguarding training (paragraph 84) and the requirement to ensure children are taught about safeguarding, including online safety (paragraph 87), that online safety training for staff is integrated, aligned and considered as part of the overarching safeguarding approach.