Royal Free Hospital Children's School
E-Safety Policy and Procedures
November 2020

CONTENT

- **Staff**

Appendix

1. **Pupil Digital Rights**
2. **Acceptable use policies for primary schools**
3. **Acceptable use policies for secondary schools**
4. **Acceptable use policies for staff**
5. **E-safety incident report form**
6. **Reporting a suspicion or disclosure flow chart**
7. **Description of ICT applications**
8. Acceptable use policy- **Online learning consent and contract (Parent & Young person)**
9. Acceptable use policy- **Online risk assessment completed by personal tutor/referring teacher**

Key contacts

ROYAL FREE HOSPITAL CHILDREN'S SCHOOL

Designated Safeguarding Lead:
Name: Jemma Michelson — Contact details: 07393626063
Name: Alex Yates (Head teacher) — Contact details: 07470370379

Deputy Designated Safeguarding Leads:
Name: James Friel — Contact details: 07811318759
Name: Lilli Lodge — Contact details: 07471807747

Designated LAC Teacher
Name: Siobhan Auberge — Contact details: 07471807747

Nominated Governor for Child Protection:
Name: Diana Goldin — Contact details: **020 7794 0500**

Location of Child Protection information and policy documents: School Office

Location of Child Protection related information: School Office

LONDON BOROUGH OF CAMDEN

Child Protection Lead officer and Local Authority Designated Officer (LADO):
Name: Sophie Kershaw Sophie.Kershaw@camden.gov.uk — Tel: 020 7974 4556/3828

Safeguarding Lead Officers:
Name: Michelle O'Regan (Head of Service – Children in Need) — Tel: 020 7974 1905

Name: Tracey Murphy (Service manager) — Tel: 020 7974 4103

Name: Patricia Williams (Service manager) — Tel: 020 7974 1558

Children's Contact Service/MASH team:
Manager: Jade Green jade.green@camden.gov.uk — Tel: 020 7974 1553/3317

Online safety contact officer:
Name: Jenni Spence Jenni.spencer@camden.gov.uk — Tel: 020 7974 2866

Prevent Education Officer
Name: Jane Murphy Jane.murphy@camden.gov.uk — Tel: 020 7974 1008

Children and Young People Disability Service
Name: Crina Popa Crina.Popa@camden.gov.uk Tel: 020 7974 4867

Virtual School
Name: Natalie White Natalie.White@camden.gov.uk Tel: 020 7974 2359

Looked After Children
Name: Sally Joseph Sally.Joseph@camden.gov.uk Tel: 020 7974 6798

DEFINITION AND PURPOSE OF E-SAFETY

E-safety forms part of the "Staying Safe" element of the Government's Every Child Matters agenda. The school has a responsibility under the Children Act 2004 to safeguard and promote the welfare of pupils, as well as owing a duty of care to children and their parents/carers to provide a safe learning environment.

Rationale

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at Royal Free Hospital Children's School with respect to the use of ICT-based technologies
- Safeguard and protect the children and staff of RFHCS
- Assist school staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the internet for educational, personal or recreational use
- Have clear structures to deal with online abuse such as cyberbullying which are cross referenced with other school policies
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken
- Minimise the risk of misplaced or malicious allegations made against adults who work with students

This policy applies to all members of The Royal Free Hospital Children's School community (including staff, pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of The Royal Free Hospital Children's School.

E-SAFETY: THE ISSUES

Introduction

Children are growing up in a world dominated by information and communications technology (ICT) that provides them with access to a wide range of information and increased opportunities for instant communication and social networking.

Using the internet can benefit children's education and give them more opportunities to socialise, but it can also present risks which should be balanced against the need to safeguard children.
Children are often unaware that they are as much at risk online as they are in the real world. Parents/carers and schools may deny or limit access to the internet; however, this often has little effect as children access the internet in a range of ways such as on mobile phones.

Information on technologies

Internet technology contains a vast store of information from all over the world which is mainly aimed at an adult audience and may be unsuitable for children. It also provides a wide range of activities that have educational use but also inherent risks for children. (See Appendix 6)

Benefits of IT

The internet can make a huge contribution to children's education and social development by -

- Raising educational attainment, engaging and motivating pupils to learn and improving their confidence
- Improving pupil's research and writing skills
- Allowing children with disabilities to overcome communications barriers
- Improving pupil's wellbeing through the social and communications opportunities offered
- Providing access to a wide range of educational materials and teaching resources.
- Giving access to information, electronic communications and social networking
- Preparing pupils for the working environment

Risks

The main areas of risk for our school community can be summarised as follow:

Content

- Exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with racist language), substance abuse or information advocating violence, racism or illegal/anti-social behaviour.
- Visiting sites that advocate extreme and dangerous behaviour such as self-harm or suicide or violent extremism, and more vulnerable children may be at a high degree of risk from such sites. All children may become desensitised to pornography, violence, sex and drug use or self-harm by regularly viewing these on-line
- Lifestyles websites, for example pro-anorexia/self-harm/suicide sites
- Hate sites
- Content validation: how to check authenticity and accuracy of online content

Contact

Chat rooms, gaming sites and other social networking sites can pose a real risk to children as users can take on an alias rather than their real names and can hide their true identity. The sites may be used by adults who pose as children in order to befriend and gain children's trust (known as "grooming") with a view to sexually abusing them.

Children may not be aware of the danger of publishing or disclosing personal information about themselves such as contact details that allow them to be identified or located. They may also inadvertently put other children at risk by posting personal information and photographs without consent. Identity theft (including 'frape' - hacking Facebook profiles) and sharing passwords

The internet may also be used as a way of bullying a child, known as online bullying or Cyber bullying

Commerce

Children are vulnerable to unregulated commercial activity on the internet that could have serious financial consequences, such as fraud or identity theft, for themselves and their parents. They may give out financial information, for example, their parent's credit card details, in response to offers for goods or services without seeing the fraudulent intent. Contact via social networking sites can also be used to persuade children to reveal computer passwords or other information about the family for the purposes of fraud.

Conduct

- Privacy issues, including disclosure of personal information and photographs, digital footprint and online reputation
- Health and well-being (amount of time spent online (internet or gaming)) that may have a negative impact on their health, social and emotional development and their educational attainment
- Use of mobile devices to take and distribute inappropriate images of the young person (sexting - sending and receiving of personally intimate images) also referred to as SGII (self generated indecent images) that cannot be removed from the internet and can be forwarded on to a much wider audience than the child intended
- Cyber bullying

Culture

Children need to be taught to use the internet in a responsible way, as they may put themselves at risk by:

- Becoming involved in inappropriate, anti-social or illegal activities as a result of viewing unsuitable materials or contact with inappropriate people
- Using information from the internet in a way that breaches copyright laws without realising they are publishing to a potentially global audience
- Uploading personal information about themselves, including photographs, on social networking sites without realising they are publishing to a potentially global audience
- Online bullying

- Use of mobile devices to take and distribute inappropriate images of the young person (sexting) that cannot be removed from the internet and can be forwarded on to a much wider audience than the child intended.

Children may also be adversely affected by obsessive use of the internet that may have a negative impact on their health, social and emotional development and their educational attainment. They may visit sites that advocate extreme and dangerous behaviour such as self-harm or suicide or violent extremism, and more vulnerable children may be at a high degree of risk from such sites. All children may become desensitised to pornography, violence, sex and drug use or self-harm by regularly viewing these on-line.

SCHOOL E-SAFETY STRATEGIES

Purpose and description

Computing is now a key part of the school curriculum and one of the key aims of computing is to ensure that pupils are aware of e-safety messages. This is part of the school's responsibility to safeguard and promote the welfare of pupils, as well as the duty of care to children and their parents to provide a safe learning environment.

Elements of e-safety

The school enables an "e-safe" environment for pupils by ensuring that the following aspects are addressed:

- Safe systems

The school is linked to the internet through the London Grid for Learning platform. Camden's Schools IT team ensures that the London Grid for Learning platform offers a safe e-learning environment by providing filtering software to block access to unsuitable sites, anti-virus software and internet monitoring systems. School also uses Google Drive to enable students to access work that has been set by the school staff. This is monitored by the Deputy Head.

- Safe practices

The school uses their e-safety policy and practice to ensure everyone is aware of the issues and knows what is expected of them in terms of their own acceptable use of the internet and other technologies. The policy is used in conjunction with the school's Anti-bullying Policy.

- Safety awareness

Pupils usually have access to the internet at home, and the school aims to keep parents/carers fully aware of e-safety issues, so they can extend e-safety strategies to the home environment. In partnership with parents/carers, the school plays an important role in raising pupils' awareness of the potential dangers of using the internet and helping them to develop their own strategies to avoid these risks and keep safe online.

Roles and responsibilities

Role	Key Responsibilities
Headteacher	• Takes overall responsibility for e-safety provision • Takes overall responsibility for data and data security (SIRO) • Ensures the school uses an approved, filtered internet Service, which complies with

	current statutory requirements e.g. The London Grid for Learning Platform • Is responsible for ensuring that staff receive suitable training to carry out their e-safety roles and to train other colleagues, as relevant • Is aware of procedures to be followed in the event of a serious e-safety incident • Receives regular monitoring reports from the e-safety Co-ordinator • Ensures that there is a system in place to monitor and support staff who carry out internal e-safety procedures (e.g. network manager) • Links with the Governing Body and parents/carers to promote e-safety and forward the school's e-safety strategy • Ensures that e-safety issues are given a high profile within the school community • Decides on sanctions against staff and pupils who are in breach of acceptable use policies
Governors / E-safety governor	The Governing Body has a statutory responsibility for pupil safety • Ensures that the school follows all current e-safety advice to keep the children and staff safe • Approves the e-safety policy and reviews the effectiveness of the policy. This will be carried out by the Governors / Governors Sub Committee receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of e-safety Governor • Supports the school in encouraging parents/carers and the wider community to become engaged in e-safety activities • The role of the e-safety Governor will include regular review with the e-safety Co-ordinator (including e-safety incident logs, filtering / change control logs) • Governors should always use business email addresses when conducting school business
E-safety Co-ordinator / Designated Child Protection Lead	• Takes day to day responsibility for e-safety issues and has a leading role in establishing implementing, monitoring and reviewing the school e-safety policies / documents • Ensures that all staff are aware of the procedures that need to be followed in the event of an e-Safety incident • Ensures that e-safety education is embedded across the curriculum • Provides the first point of contact and advice for school staff, governors, pupils and parents/carers • Liaise with the school's network manager, the head teacher and nominated governor to ensure the school remains up to date with online safety issues and to address any new trends, incidents and arising problems • Is regularly updated in e-safety issues and legislation, and be aware of the potential for serious child protection issues to arise from: o sharing of personal data o access to illegal / inappropriate materials o inappropriate on-line contact with adults / strangers o potential or actual incidents of grooming o cyber-bullying and use of social media • Assesses the impact and risk of emerging technology and the school's response to this in association with staff • Promotes an awareness and commitment to e-safeguarding throughout the school community • Facilitates training and advice for all staff and directs them to relevant e-safety literature • Ensures that all staff and pupils have read and signed the acceptable use policy (AUP) and pupil digital rights form • Communicates regularly with SLT and the designated e-safety Governor to discuss current issues, review incident logs and filtering / change control logs • Reports annually to the Governing Body on the implementation of the school's e-safety strategy • Ensures that the e-safety incident log is kept up to date • Liaises with the Local Authority and relevant agencies • Reports all incidents and issues to Camden's e-safety officer

	Where an e-safety incident has serious implications for the child's safety or well-being, the matter will be referred to the designated Child Protection teacher, who will decide whether or not a referral should be made to Safeguarding and Social Care, or the Police.
Network Manager	• Ensures that provision exists for misuse detection and malicious attack (e.g. keeping virus protection up to date) • Reports any e-safety related issues that arise, to the e-safety coordinator • Ensures that the use of the network / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the e-safety Co-ordinator /Headteacher for investigation / action / sanction • Ensures that users may only access the school's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed • Ensures the security of the school ICT system • Ensures that access controls / encryption exist to protect personal and sensitive information held on school-owned devices • Ensures the school's policy on web filtering is applied and updated on a regular basis • Ensures that the London Grid for Learning platform is informed of issues relating to the filtering applied by the Grid • Keeps up to date with the school's e-safety policy and technical information in order to effectively carry out their e-safety role and to inform and update others as relevant • Ensures appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster • Keeps up-to-date documentation of the school's e-security and technical procedures • Supports any subsequent investigation into breaches and preserving any evidence.
Learning Platform Leader	• Ensures that all data held on pupils on the London Grid for Learning platform is adequately protected
Data Manager	• Ensures that all data held on pupils on the school office machines have appropriate access controls in place
London Grid for Learning platform Nominated contact(s)	• Ensures all London Grid for Learning platform services are managed on behalf of the school including maintaining the London Grid for Learning platform USO database of access accounts
Computing Curriculum Leader	• Oversees the delivery of the e-safety element of the Computing curriculum • Liaises with the e-safety coordinator regularly
Teachers	• Adhere to the school's e-safety and acceptable use policy and procedures • Communicate the school's e-safety, acceptable use policy and pupil digital rights form to pupils • Embed e-safety issues in all aspects of the curriculum and other school activities • Supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extracurricular and extended school activities if relevant) • Ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws • Report breaches of internet use to the e-safety officer • Recognise when pupils are at risk from their internet use or have had negative experiences and taking appropriate action, e.g. referral to the e-safety contact officer • Teach the e-safety and digital literacy elements of the new curriculum
All staff	• Read, understand and help promote the school's e-safety policies and guidance • Read, understand, sign and adhere to the school staff Acceptable Use Agreement • Are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices • Keep pupils safe and ensure they receive appropriate supervision and support whilst using the internet

	• Report any suspected misuse or problem to the e-safety coordinator • Maintain an awareness of current e-safety issues and guidance e.g. through CPD • Model safe, responsible and professional behaviours in their own use of technology • Ensure that any digital communications with pupils should be on a professional level and only through school based systems, never through personal mechanisms, e.g. email, text, mobile phones • Use Google Drive to enable students to access work that has been set by the school staff
Pupils	• Read, understand, sign and adhere to the Student Acceptable Use Policy and the pupil digital rights form • Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations • Understand the importance of reporting abuse, misuse or access to inappropriate materials • Know what action to take if they or someone they know feels worried or vulnerable when using online technology • Know and understand school policy on the use of mobile phones, digital cameras and hand held devices • Know and understand school policy on the taking / use of images and on cyber-bullying • Understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's e-safety policy covers their actions out of school, if related to their membership of the school • Take responsibility for learning about the benefits and risks of using the internet and other technologies safely both in school and at home • Help the school in the creation/ review of e-safety policies
Pupil's with special educational needs and disabilities (SEND	Pupils with learning difficulties or disability may be more vulnerable to risk from use of the internet and may need additional guidance on online safety practice as well as closer supervision. SEND co-ordinator is responsible for providing extra support for these pupils and should: • Link with the online safety co-ordinator to discuss and agree whether the mainstream safeguarding systems on the internet are adequate for pupils with SEND • Where necessary, liaise with the online safety co-ordinator and the IT service to discuss any requirements for further safeguards to the school IT system or tailored resources and materials in order to meet the needs of pupils with SEND • Ensure that the school's online safety policy is adapted to suit the needs of pupils with SEND • Liase with parents, carers and other relevant agencies in developing online safety practices for pupils with SEND • Keep up to date with any developments regarding emerging technologies and online safety and how these may impact on pupils with SEND.
Parents/carers	• Support the school in promoting e-safety and endorse the Parents' Acceptable Use Agreement which includes the pupils' use of the internet and the school's use of photographic and video images • Read, understand and promote the school Pupil Acceptable Use Agreement and the pupil digital rights form with their children • Access the school website / London Grid for Learning platform / on-line student / pupil records in accordance with the relevant school Acceptable Use Agreement • Consult with the school if they have any concerns about their children's use of technology • Admission packs contain information on the school's e-safety policy and Acceptable Use agreement • Should refer to the following online safety leaflet for guidance https://www.cscb-new.co.uk/wp-content/uploads/2017/03/Online_Safety_Leaflet_for_Parents.pdf
External groups	• Any external individual / organisation will sign an Acceptable Use Policy prior to using any equipment or the internet within school

How will this policy be communicated?

It will be communicated in the following ways:

- Posted on the Royal Free Hospital children's School website
- Available on the internal staff network/drive
- Available in paper format in all Royal Free sites:
    - The Hive
    - QMH- EDIS school room
    - Royal Free Hospital
- Part of school induction pack for all new staff (including temporary, supply and non-classroom-based staff)
- Integral to safeguarding updates and training for all staff (especially in September refreshers)
- Clearly reflected in the Acceptable Use Policies (AUPs) for staff, volunteers, contractors, governors, pupils and parents/carers (which must be in accessible language appropriate to these groups).
- AUPs issued to whole school community, on entry to the school, with annual reminders of where to find them if unchanged, and reissued if updated after annual review
- Reviews of this online-safety policy will include input from staff, pupils and other stakeholders, helping to ensure further engagement
- Acceptable use agreements to be held in pupil and personnel files

E-SAFETY POLICIES

Accessing and monitoring the system

- Access to the London Grid for Learning platform for pupils and staff is via individual log-ins and passwords. Visitors should have permission from the head teacher or e-safety contact officer to access the system and be given a separate visitors log-in
- A record of all log-ins used within the school is kept by Camden LA for the purposes of monitoring and auditing internet activity
- Staff should be required to change their password every 6 months.
- Camden's Schools IT team is responsible for the school's Technician and monitoring the system and should be supervised by a senior member of their management team
- The school has carefully considered the location of computer terminals in the classroom, in order to allow an appropriate level of supervision of pupils depending on their age and experience

Confidentiality and data protection

- The school will ensure that all data held on its IT systems is held in accordance with the principles of the Data Protection Act 2018. Data will be held securely and password protected with access given only to staff members on a "need to know" basis.
- Pupil data that is being sent to other organisations will be encrypted and sent via a safe and secure system such as School2School. Any breaches of data security should be reported to the head teacher immediately.
- Where the school uses CCTV, a notice will be displayed in a prominent place to ensure staff and students are aware of this and recordings will not be revealed without appropriate permission

Personal data and GDPR

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

"GDPR does not prevent, or limit, the sharing of information for the purposes of keeping children safe. Lawful and secure information sharing between schools, Children's Social Care, and other local agencies, is essential for keeping children safe and ensuring they get the support they need. The Data Protection

Act 2018 introduced 'safeguarding' as a reason to be able to process sensitive, personal information, even without consent (DPA, Part 2,18; Schedule 8, 4) When Designated Safeguarding Leads in schools are considering whether, or not, to share safeguarding information (especially with other agencies) it is considered best practice for them to record who they are sharing that information with and for what reason. If they have taken a decision not to seek consent from the data subject and/or parent/carer that should also be recorded within the safeguarding file. All relevant information can be shared without consent if to gain consent would place a child at risk. Fears about sharing information must not be allowed to stand in the way of promoting the welfare and protecting the safety of children."

All pupils, staff, governors, volunteers, contractors and parents are bound by the school's data protection policy and agreements

The headteacher/principal, data protection officer and governors work together to ensure a GDPR-compliant framework for storing data, but which ensures that child protection is always put first and data-protection processes support careful and legal sharing of information.

Staff are reminded that all safeguarding data is highly sensitive and should be treated with the strictest confidentiality at all times, and only shared via approved channels to colleagues or agencies with appropriate permissions.

Cloud Platforms

It is important to consider data protection before adopting a cloud platform. The Royal Free Hospital Children's School uses Google for Education's G Suite, myDrive for file storage, etc]

For online safety, basic rules of good password hygiene ("Treat your password like your toothbrush –never share it with anyone!"), expert administration and training can help to keep staff and pupils safe, and to avoid incidents

The following principles apply:

- Privacy statements inform parents and children (13+) when and what sort of data is stored in the cloud
- The DPO approves new cloud systems, what may or may not be stored in them and by whom. This is noted in a DPIA (data-protection impact statement) and parental permission is sought
- Regular training ensures all staff understand sharing functionality and this is audited to ensure that pupil data is not shared by mistake. Open access or widely shared folders are clearly marked as such
- Pupils and staff are only given access and/or sharing rights when they can demonstrate an understanding of what data may be stored and how it can be seen
- Two-factor authentication is used for access to staff or pupil data
- Pupil images/videos are only made public with parental permission
- Only school-approved platforms are used by students or staff to store pupil work
- All stakeholders understand the difference between consumer and education products (e.g. a private Gmail account or Google Drive and those belonging to a managed educational domain)

Acceptable Use Policy

- All London Grid for Learning platform users within the school will be expected to sign an acceptable use agreement that sets out their rights and responsibilities and incorporates the school e-safety rules regarding their internet use
- For primary school pupils, acceptable use agreements will be signed by parents/carers on their child's behalf at the same time that they give consent for their child to have access to the London Grid for Learning platform in school (See Appendix 1 & 3)
- Secondary school pupils and their parents/carers should both sign the acceptable use policy and the Pupil Digital Rights, and use of the London Grid for Learning platform in schools is dependent on signing this agreement (See Appendix 2 & 3)

- Staff are expected to sign an acceptable use policy on appointment and this will be integrated into their general terms of employment (See Appendix 4)
- The Headteacher will keep a copy of all signed acceptable use agreements.

Digital Images and video

When a pupil/student joins the school, parents/carers are asked if they give consent for their child's image to be captured in photographs or videos, in the admissions pack on entry into the Royal Free Hospital Children's school.

Digital images and videos may be used for:

- For displays around the school
- For the newsletter
- For use in paper-based school marketing
- For online prospectus or websites
- For a specific high profile image for display or publication
- School website

Whenever a photo or video is taken/made, the member of staff taking it will check the latest database before using it for any purpose.

Any pupils shown in public facing materials are never identified with more than first name (and photo file names/tags do not include full names to avoid accidentally sharing them).

All staff are governed by their contract of employment and the school's Acceptable Use Policy, which covers the use of mobile phones/personal equipment for taking pictures of pupils, and where these are stored.

At The Royal Free Hospital Children's school, no member of staff will ever use their personal phone to capture photos or videos of pupils.

Photos are stored on the school network, Google classroom in line with the retention schedule of the school Data Protection Policy.

Staff and parents are reminded regularly about the importance of not sharing without permission, due to reasons of child protection (e.g. looked-after children often have restrictions for their own protection), data protection, religious or cultural reasons, or simply for reasons of personal privacy.

We encourage young people to think about their online reputation and digital footprint, so we should be good adult role models by not oversharing (or providing embarrassment in later life – and it is not for us to judge what is embarrassing or not).

Pupils are taught about how images can be manipulated in their online safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children

Pupils are advised to be very careful about placing any personal photos on social media. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.

Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location. We teach them about the need to keep their data secure and what to do if they / or a friend are subject to bullying or abuse.

Social Media

Alex Yates, **Head teacher at the Royal Free Hospital Children's school** is responsible for managing the schools website, Twitter Google Plus accounts and checking our Wikipedia and Google reviews.

Staff, pupils' and parents use of Social media

Social media (including here all apps, sites and games that allow sharing and interaction between users) is a fact of modern life, and as a school, we accept that many parents, staff and pupils will use it. However, as stated in the acceptable use policies which all members of the school community sign, we expect everybody to behave in a positive manner, engaging respectfully with the school and each other on social media, in the same way as they would face to face.

This positive behaviour can be summarised as not making any posts which are or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which might bring the school or (particularly for staff) teaching profession into disrepute. This applies both to public pages and to private posts, e.g. parent chats, pages or groups.

If parents have a concern about the school, we would urge them to contact us directly and in private to resolve the matter. If an issue cannot be resolved in this way, the school complaints procedure should be followed. Sharing complaints on social media is unlikely to help resolve the matter, but can cause upset to staff, pupils and parents, also undermining staff morale and the reputation of the school (which is important for the pupils we serve).

Many social media platforms have a minimum age of 13 (note that WhatsApp is 16. We ask parents to respect age ratings on social media platforms wherever possible and not encourage or condone underage use. It is worth noting that online harms regulation is likely to require more stringent age verification measures over the coming years

.

However, the school has to strike a difficult balance of not encouraging underage use at the same time as needing to acknowledge reality in order to best help our pupils/students to avoid or cope with issues if they arise. Online safety lessons will look at social media and other online behaviour, how to be a good friend online and how to report bullying, misuse, intimidation or abuse. However, children will often learn most from the models of behaviour they see and experience, which will often be from adults.

Parents can best support this by talking to their children about the apps, sites and games they use (you don't need to know them – ask your child to explain it to you), with whom, for how long, and when (late at night / in bedrooms is not helpful for a good night's sleep and productive teaching and learning at school the next day).

Using Social media to communicate:

Pupils/students are not allowed* to be 'friends' with or make a friend request** to any staff, governors, volunteers and contractors or otherwise communicate via social media.

Pupils/students are discouraged from 'following' staff, governor, volunteer or contractor public accounts (e.g. following a staff member with a public Instagram account). However, we accept that this can be hard to control (but this highlights the need for staff to remain professional in their private lives). In the reverse situation, however, staff must not follow such public student accounts.

** Exceptions may be made, e.g. for pre-existing family links, but these must be approved by the Headteacher/Principal, and should be declared upon entry of the pupil or staff member to the school).*

*** Any attempt to do so may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the Headteacher (if by a staff member).*

Staff are reminded that they are obliged not to bring the school or profession into disrepute and the easiest way to avoid this is to have the strictest privacy settings and avoid inappropriate sharing and oversharing online. They should never discuss the school or its stakeholders on social media and be careful that their personal opinions might not be attributed to the school, trust or local authority, bringing the school into disrepute.

The serious consequences of inappropriate behaviour on social media are underlined by the fact that of the 131 Prohibition Orders issued to staff in 2017, 73 involved social media/technology (and 27 of the 66 orders by August 2018).

All members of the school community are reminded that particularly in the context of social media, it is important to comply with the school policy on Digital Images and Video (see page **Error! Bookmark not defined.**) and permission is sought before uploading photographs, videos or any other information about other people.
The statements of the Acceptable Use Policies (AUPs) which all members of the school community have signed are also relevant to social media activity, as is the school's Data Protection Policy.

Personal Devise usage
Remind those with access to school devices about rules on the misuse of school technology – devices used at home should be used just like if they were in full view of a teacher or colleague. Please read the following in conjunction with acceptable use policies and the following sections of this document which all impact upon device usage: copyright, data protection, social media, misuse of technology, and digital images and video.

- **Pupils/students** in Year 10 and 11 are allowed to bring mobile phones in for emergency use only / may use mobile phones during lunch break, but not when moving around the school buildings. Pupils hand their devices in to the school business manager at the beginning of the school day. They are returned at the end of the school day. Any attempt to use a phone in lessons without permission or to take illicit photographs or videos will lead to sanctions as outlined in the behaviour policy- parents will also be informed. Important messages and phone calls to or from parents can be made with the school business manager, which will also pass on messages from parents to pupils in emergencies.
- **All staff who work directly with children** should leave their mobile phones on silent and only use them in private staff areas during school hours. Child/staff data should never be downloaded onto a private phone. If a staff member is expecting an important personal call when teaching or otherwise on duty, they may leave their phone with the school office to answer on their behalf or ask for the message to be left with the school office.
- **Volunteers, contractors, governors** should leave their phones in their pockets and turned off. Under no circumstances should they be used in the presence of children or to take photographs or videos. If this is required (e.g. for contractors to take photos of equipment or buildings), permission of the headteacher should be sought (the headteacher may choose to delegate this) and this should be done in the presence of a member staff.
- **Parents** are asked to leave their phones in their pockets and turned off when they are on site. They should ask permission before taking any photos, e.g. of displays in corridors or classrooms, and avoid capturing other children. Parents are asked not to call pupils on their mobile phones during the school day; urgent messages can be passed via the school business manager.

Network/Internet access on school devices

- **Pupils/students** are not allowed networked file access via personal devices. However, they are allowed to access the school wireless internet network for school-related internet use / limited personal use within the framework of the acceptable use policy. All such use is monitored.
- **Home devices** are issued to some students. These are restricted to the apps/software installed by the school and may be used for learning and reasonable and appropriate personal use at home, but all usage may be tracked.
- **All staff who work directly with children** should leave their mobile phones on silent and only use them in private staff areas during school hours. Child/staff data should never be downloaded onto a private phone.

- **Volunteers, contractors, governors** have no access to the school network or wireless internet on personal devices . All internet traffic is monitored.
- **Parents** have no access to the school network or wireless internet on personal devices

Teaching e-safety

Responsibility

One of the key features of the school's online safety strategy is teaching pupils to protect themselves and behave responsibly while on-line. There is an expectation that over time, pupils will take increasing responsibility for their own behaviour and internet use so that they can be given more freedom to explore systems and applications with a lessening amount of supervision from staff.

- Overall responsibility for the design and co-ordination of online safety education lies with the head teacher and the online safety co-ordinator, but all staff should play a role in delivering online safety messages
- The online safety co-ordinator is responsible for ensuring that all staff have the knowledge and resources to enable them to carry out this role
- One of the key features of the school's e-safety strategy is teaching pupils to protect themselves and behave responsibly while online.
- Teachers are primarily responsible for delivering an ongoing online safety education in the classroom as part of the curriculum
- Rules regarding safe internet use should be posted up in all classrooms and teaching areas where computers are used to deliver lessons
- The start of every lesson where computers are being used should be an opportunity to remind pupils of expectations on internet use and the need to follow basic principles in order to keep safe
- Teachers may wish to use PSHE lessons and Collective Time as forums for discussion on online safety issues to ensure that pupils understand the risks and why it is important to regulate their behaviour whilst on-line
- Teachers should be aware of those children who may be more vulnerable to risk from internet use, generally those children with a high level of experience and good computer skills but coupled with poor social skills
- Teachers should ensure that the school's policy on pupils' use of their own mobile phones and other mobile devices in school is adhered to.

Remote learning policy 2020

Remote learning for pupils that are not able to attend school due to self-isolation or in line with government guidelines

- The Royal Free Hospital school will provide remote learning (online) for pupils that are not able to attend school so that no-one need fall to far behind.
- The Royal Free Hospital school are fully aware that these are exceptional times and that this document seeks to inform and guide families and not impose expectations. Each family is unique and because of this, should approach home learning in way which suits their individual needs.
- Where possible, it is beneficial for young people to maintain a regular and familiar routine. We recommend that in the event that a pupil is accessing education remotely, each 'school day' maintains structure, following the weekly timetable already established at the Royal Free Hive day school offering a full program of study.
- Using the online platform of Google class room, the Royal free Hospital Children's school are able to offer a 'live stream' for pupils to engage and be interactive in lessons in the event that pupils are unable to attend school.
- Learning in this way, pupils can join and follow all lessons as if they were present for the school day.
- Pupils are issued with an individual login email address, username and password, which is completely unique to them. On their Google profile, pupils can use the individual google drive area

to save their work securely, create google documents as well as engage with teachers in the comment section for feedback to their work which has been submitted.

- Royal free school subject teachers will post lesson resources, slides, handouts, any worksheets and homework in their specific classroom area for pupils to access.
- Every effort will be made by staff to ensure that work is set promptly on appropriate platforms but school cannot guarantee that the chosen platforms will work on all devices. Should accessing work be an issue, parents should contact school promptly and alternative solutions may be available. These will be discussed on case-to-case basis.
- Should anything be unclear in the work that is set, parents can communicate with class teachers via the school email address; admin@royalfree.camden.sch.uk.

Key responsibilities:
All stakeholders in the Royal Free school have a responsibility to follow policies, rules and procedures to ensure the safe use of online platforms for the purpose of successful online learning.

Teachers & Volunteers:

- Read, understand, sign and adhere to an acceptable use policy (AUP)
- Report any concerns, no matter how small, to the designated safety lead / online safety coordinator as named in the AUP
- Maintain an awareness of current online safety issues and guidance
- Model safe, responsible and professional behaviours in their own use of technology at school and as part of remote teaching or any online communications
- A Volunteer will never attempt to arrange any meeting, **including teaching session,** without the full prior knowledge and approval of the school, and will never do so directly with a pupil. The same applies to any private/direct communication with a pupil.

Pupils:

- Read, understand, sign and adhere to the student/pupil acceptable use policy for remote learning and review this annually
- Treat **home learning during any isolation/quarantine or bubble/school lockdown** in the same way as regular learning in school and behave as if a teacher or parent were watching the screen
- Avoid any private communication or use of personal logins/systems to communicate with or arrange meetings with school staff or members of staff working in the school.
- Understand the importance of reporting abuse, misuse or access to inappropriate materials, including any concerns about a member of school staff or supply teacher or online tutor
- Know what action to take if they or someone they know feels worried or vulnerable when using online technology, at school, home or anywhere else.
- To understand the importance of adopting safe and responsible behaviours and good online safety practice when using digital technologies outside of school and realise that the school's acceptable use policies cover actions out of school, including on social media
- Remember the rules on the misuse of school technology – devices and logins used at home should be used just like if they were in full view of a teacher.
- Understand the benefits/opportunities and risks/dangers of the online world and know who to talk to at school or outside school if there are problems

Parents/Carers:

Read, sign and promote the school's parental acceptable use policy (AUP) and read the pupil AUP and encourage their children to follow it

- Consult with the school if they have any concerns about their children's and others' use of technology

- Promote positive online safety and model safe, responsible and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers.
- Encourage children to engage fully in home-learning during any period of isolation/quarantine or bubble/school closure and flag any concerns
- Support the child during remote learning to avoid video calls in a bedroom if possible and if not, to ensure the child is fully dressed and not in bed, with the camera pointing away from beds/bedding/personal information etc. and the background blurred or changes where possible.
- If organising private online tuition, remain in the room if possible, ensure the child knows tutors should not arrange new sessions directly with the child or attempt to communicate privately.

External groups/Parent associations/Governors:

- Any external individual/organisation will sign an acceptable use policy prior to using technology or the internet within school
- Support the school in promoting online safety and data protection
- Model safe, responsible, respectful and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers

Online learning Platforms:
Using different online platforms to engage young people in remote learning. The royal free school uses a variety of different remote learning platforms to engage young people between the ages of 5-16 years old.

These include:

- Zoom
    - **Zoom** - Only use accounts set up by school admins. If you consider Zoom, please use the paid education version, not a free account, for the ability to safely audit staff and student meeting behaviour, record or disable chat, and other essential safeguarding settings.

- Google Suite
    - **Google Meet within G Suite** - there are many settings in G Suite to help you use Meet safely, e.g. disable chat, choose between a video meeting and a stream,

    - Teachers should only start a Meet or stream and students can only join the, audit staff-pupil contacts and many more essential safeguards. **NB -** to **stop students rejoining a Meet without the teacher there**, you must start it from meet.google.com ***AND give it a name*** (not via calendar which is the only place to schedule a stream).

    - There are now **Google Classroom-linked Meet rooms** which are the best option to make sure only students in the relevant class can join a Meet and only when a teacher has started it.

    - **YouTube -** teachers should never use personal channels/accounts, but only those linked to a school's G Suite. **Google Meet is a better solution** for live lessons, assemblies or meetings

- Microsoft Teams for professional meetings
    - **Microsoft Teams within Office 365** - This Microsoft page includes a really helpful list of recommended safe settings. **NB -** to **stop students rejoining a Teams call without the teacher there**, you must click End Meeting, not the classic 'hang up' button.

Safeguarding Considerations for Lesson Livestreaming:

- Has parental/carer consent been given for a pupil to engage online in remote learning?
- Has the pupil themselves read and signed the 'rules and expectations' consent form before online learning has begun?
- Have teachers completed risk assessment for vulnerable young people in the class?
- Have SEND needs been considered to engage all pupils in inclusive learning in this way?
- Teaching staff should only use school-registered accounts, never personal ones- approved by SLT
- Will some students be excluded? Do they have internet, a device and a quiet place?
- How will inclusive teaching be facilitated? How will teachers support vulnerable students with SEND and CP needs?
- Have the settings in the online platform been pre-set by admin? (who can chat? who can start a stream? who can join?)
- Ensure the link isn't public for the whole world to see
- Do students and staff have a safe and appropriate place to do the lesson? Are there any inappropriate objects/information visible in the background?
- Don't turn on streaming for students by mistake – joining a stream /starting a stream
- Never start without another member of staff in the 'room' and without other colleagues aware you are having a lesson with a young person
- Avoid one-to-one lessons unless pre-approved by SLT
- Keep a log of everything - what, when, with whom and anything that went wrong- feedback this to DSL & personal tutor for the young person
- Remind pupils and staff about the consent/rules agreements they have signed
- Remind pupils and staff about the safeguarding policy and reporting process – does it work remotely?
- Gather consent from parents/carers in the event young people or adults do not want you want to be recorded it?
- Are students secretly recording lessons? What to do in the event this takes place
- How will pupils know when can they can speak ?
- How can students ask questions or get help?
- Will the chat function be turned on for pupils? Can pupils chat when teachers aren't there?

<u>Communicating with parents, carers and pupils</u>

Where education is having to take place remotely due to coronavirus (COVID-19), it's important for schools, teachers and pupils to maintain professional practice as much as possible. When communicating online with parents and pupils, the Royal Free school 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
- advise teachers not to share personal information

<u>Virtual lessons and live streaming</u>

The Royal Free school proves education using live streaming via Google Class room and/or Zoom platforms.

Teaching from home is different from teaching in the classroom. Teachers should try to find a quiet or private room or area to talk to pupils, parents or carers. When broadcasting a lesson or making a recording, all teachers will

<u>Providing pastoral care remotely</u>

Where pupils are required to remain at home (for example, if pupils need to self-isolate or there are local restrictions) helping parents, carers and pupils to make a weekly plan or structure is important. These plans

should include time for education, playing and relaxing to reduce stress and anxiety. Routine can give children and young people an increased feeling of safety in the context of uncertainty.

One-to-one sessions could be appropriate in some circumstances, however where possible group lessons are preferred. For example, to provide pastoral care or provide support for pupils with special educational needs and disabilities (SEND). One to one sessions, without the inclusion of a third adult in the virtual room, should be discussed and approved by the senior leadership team to assess any risks. Where possible, including a parent or additional staff member in the call is the preferred option for all engagement with young people online. This is noted in the parent/carer & pupil consent agreement prior to engaging with remote learning.

Pupil e-Safety curriculum

The Royal Free Hospital Children's School

- Has a clear, progressive e-safety education programme as part of the Computing and PSHE curriculum. It is built on LA e-safeguarding and national guidance. This covers a range of skills and behaviours appropriate to their age and experience, including:
    - To STOP and THINK before they CLICK
    - To develop a range of strategies to evaluate and verify information before accepting its accuracy
    - To be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be
    - To know how to narrow down or refine a search
    - To understand how search engines work and to understand that this affects the results they see at the top of the listings [for older pupils]
    - To understand acceptable behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private
    - To understand how photographs can be manipulated and how web content can attract the wrong sort of attention
    - To understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments
    - To understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings
    - To understand why they must not post pictures or videos of others without their permission
    - To know not to download any files – such as music files - without permission
    - To have strategies for dealing with receipt of inappropriate materials
    - To understand why and how some people will 'groom' young people for sexual reasons [for older pupils]
    - To understand the impact of cyberbullying, sexting and trolling and know how to seek help if they are affected by any form of online bullying
    - To know how to report any abuse including cyberbullying; and how to seek help if they experience problems when using the internet and related technologies, i.e. parent or carer, teacher or trusted staff member, or an organisation such as Childline or the CLICK CEOP button
- Plans internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas
- Will remind students about their responsibilities through an end-user Acceptable Use Policy which every student will sign and is also displayed throughout the school
- Ensures staff will model safe and responsible behaviour in their own use of technology during lessons
- Ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright
- Ensures that staff and pupils understand the issues around aspects of the commercial use of the internet, as age appropriate. This may include, risks in pop-ups; buying on-line; on-line gaming / gambling

Teaching about online safety

Pupils should be taught:

- The benefits and risks of using the internet
- How their behaviour can put themselves and others at risk
- What strategies they can use to keep themselves safe
- What to do if they are concerned about something they have seen or received via the internet
- Who to contact to report concerns
- That the school has a "no blame" policy so that pupils are encouraged to report any e-safety incidents
- That the school has a "no tolerance" policy regarding cyber bullying
- The basic principles of "netiquette"
- That behaviour that breaches acceptable use policies will be subject to sanctions and disciplinary action
- That the internet should only be used for educational purposes
- The London Grid for Learning platform has been designed so that use is monitored and that access to some sites is blocked
- The school's policy on using their mobile phones whilst in school.

Underpinning knowledge and behaviours

The online world develops and changes at great speed. New opportunities, challenges and risks are appearing all the time. This can make it difficult for schools to stay up to date with the latest devices, platforms, apps, trends and related threats.

It is therefore important to focus on the underpinning knowledge and behaviours that can help pupils to navigate the online world safely and confidently regardless of the device, platform or app. These lessons could be specific online safety lessons and/or school wide approaches. Teaching content will be age and developmentally appropriate.

Underpinning knowledge and behaviours include:

How to evaluate what pupils see online - This will enable pupils to make judgements about what they see online and not automatically assume that what they see is true, valid or acceptable.

Pupils should consider questions including:

- Is this website/URL/email fake? How can I tell?
- what does this cookie do and what information am I sharing?
- is this person who they say they are?
- why does someone want me to see this?
- why does someone want me to send this?
- why would someone want me to believe this?
- why does this person want my personal information?
- what's behind this post?
- is this too good to be true?
- is this fact or opinion?

How to recognise techniques used for persuasion – This will enable pupils to recognise the techniques that are often used to persuade or manipulate others. Understanding that a strong grasp of knowledge across many areas makes people less vulnerable to these techniques and better equipped to recognise and respond appropriately to strongly biased intent or malicious activity.

Help pupils to recognise:

- online content which tries to make people believe something false is true and/or mislead (misinformation and disinformation),
- techniques that companies use to persuade people to buy something,

- ways in which games and social media companies try to keep users online longer (persuasive/sticky design); and
- criminal activities such as grooming.

Online behaviour – This will enable pupils to understand what acceptable and unacceptable online behaviour look like. Schools should teach pupils that the same standard of behaviour and honesty apply on and offline, including the importance of respect for others. Schools should also teach pupils to recognise unacceptable behaviour in others.

Help pupils to recognise acceptable and unacceptable behaviour by:

- Looking at why people behave differently online, for example how anonymity (you do not know me) and invisibility (you cannot see me) affect what people do,
- looking at how online emotions can be intensified resulting in mob mentality,
- teaching techniques (relevant on and offline) to defuse or calm arguments, for example a disagreement with friends, and disengage from unwanted contact or content online; and
- considering unacceptable online behaviours often passed off as so-called social norms or just banter. For example, negative language that can be used, and in some cases is often expected, as part of online gaming and the acceptance of misogynistic, homophobic and racist language that would never be tolerated offline.
- Mob mentality describes how people can be influenced by their peers to adopt certain behaviours on a largely emotional, rather than rational, basis

How to identify online risks – This will enable pupils to identify possible online risks and make informed decisions about how to act. This should not be about providing a list of what not to do online. The focus should be to help pupils assess a situation, think through the consequences of acting in different ways and decide on the best course of action.

Help pupils to identify and manage risk by:

- discussing the ways in which someone may put themselves at risk online,
- discussing risks posed by another person's online behaviour,
- discussing when risk taking can be positive and negative,
- discussing "online reputation" and the positive and negative aspects of an online digital footprint. This could include longer-term considerations, i.e how past online behaviours could impact on their future, when applying for a place at university or a job for example,
- discussing the risks vs the benefits of sharing information online and how to make a judgement about when and how to share and who to share with; and
- asking questions such as what might happen if I post something online? Who will see it? Who might they send it to?

How and when to seek support – This will enable pupils to understand safe ways in which to seek support if they are concerned or upset by something they have seen online.

Support pupils by:

- helping them to identify who trusted adults are,
- looking at the different ways to access support from the school, police, the National Crime Agency's Click CEOP reporting service for children and 3rd sector organisations such as Child line and Internet Watch Foundation. This should link to wider school policies and processes around reporting of safeguarding and child protection incidents and concerns to school staff (see Keeping Children Safe in Education);
- helping pupils to understand that various platforms and apps will have ways in which inappropriate contact or content can be reported.

Staff and Governor training

The Royal Free Hospital Children's School:

- Ensures staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection
- Makes regular training available to staff on e-safety issues and the school's e-safety education program through termly staff meetings
- Provides, as part of the induction process, all new staff [including those on university/college placement and work experience] with information and guidance on the e-safeguarding policy and the school's Acceptable Use Policies
- Ensures that Staff attend specific training on online safety available from the CSCB so that they are aware of the risks and actions to take to keep pupils safe online. School management should ensure that staff attend regular update training in order to ensure they can keep up with new developments in technology and any emerging safety issues.

Delivering e-safety messages

- Teachers are primarily responsible for delivering an ongoing e-safety education in the classroom as part of the curriculum.
- These lessons could be specific online safety lessons and/or school wide approaches. Teaching content will be age and developmentally appropriate.
- Rules regarding safe internet use are displayed in the classroom, playroom, adolescent room and on the ward
- Each time pupils use a computer, they should be reminded of expectations on internet use and the need to follow basic principles in order to keep safe

ICT and safe teaching practice

School staff need to be aware of the importance of maintaining professional standards of behaviour with regards to their own internet use, particularly in relation to their communications with pupils, to ensure their behaviour is not open to misinterpretation and to safeguard them from misplaced or malicious allegations.

- Photographic and video images of pupils should only be taken by staff in connection with educational purposes, e.g. school trips
- Staff should always use school equipment and only store images on the school computer system, with all other copies of the images erased
- Staff should take care regarding the content of and access to their own social networking sites and ensure that pupils and parents/carers cannot gain access to these
- Staff should ensure that any materials published on their own social networking sites are neither inappropriate nor illegal
- Staff should be particularly careful regarding any comments to do with the school or specific pupils that are communicated over the internet; remarks that are private may go to a wider audience and raise questions regarding confidentiality
- Staff should not post any comments about specific pupils or staff members on their social networking sites or any comments that would bring the school or their profession into disrepute.
- Staff should not engage in any conversation with pupils via instant messaging or social networking sites as these may be misinterpreted or taken out of context
- Where staff need to communicate with pupils regarding school work, this should be via the London Grid for Learning platform or Google Drive and messages should be carefully written to ensure that they are clear, unambiguous and not open to any negative interpretation
- When making contact with parents/carers or pupils by telephone, staff should only use school equipment. Personal email addresses and accounts should never be used. Pupil or parent numbers should not be stored on a staff member's personal mobile phone and staff should avoid lending their mobile phones to pupils
- Staff should ensure that personal data relating to pupils is stored securely and encrypted if taken off the school premises
- Where staff are using mobile equipment such as laptops provided by the school, they should ensure that the equipment is kept safe and secure at all times

Exit strategy

When staff leave, their line manager should liaise with the network manager to ensure that any school equipment is handed over and that PIN numbers, passwords and other access codes to be reset so that the staff member can be removed from the school's IT system.

Safe use of Technology

Internet and search engines

- When using the internet, children should receive the appropriate level of supervision for their age and understanding. Teachers should be aware that often, the most computer-literate children are the ones who are most at risk
- Primary pupils should be supervised at all times when using the internet. Although supervision of secondary school pupils will be more flexible, teachers should remain vigilant at all times during lessons
- Pupils should not be allowed to aimlessly "surf" the internet and all use should have a clearly defined educational purpose
- Despite filtering systems, it is still possible for pupils to inadvertently access unsuitable websites; to reduce risk, teachers should plan use of internet resources ahead of lessons by checking sites and storing information off-line where possible
- Where teachers require access to blocked websites for educational purposes, this should be discussed and agreed with the e-safety contact officer, who will liaise with the Schools IT team for temporary access. Teachers should notify the e-safety contact officer once access is no longer needed to ensure the site is blocked

Evaluating and using internet content

Teachers should teach pupils good research skills that help them to maximise resources available on the Internet so that they can use search technologies effectively, appreciate how results are selected and ranked, and be discerning in evaluating digital content. They should also be taught how to critically evaluate the information retrieved by:

- Questioning the validity of the source of the information; whether the author's view is objective and what authority they carry
- Carrying out comparisons with alternative sources of information
- Considering whether the information is current and whether the facts stated are correct

In addition, pupils should be taught the importance of respecting copyright and correctly quoting sources and told that plagiarism is against the rules of the school and may lead to disciplinary action.

Safe use of applications

School email systems should be hosted by an email system that allows content to be filtered and allow pupils to send emails to others within the school or to approved email addresses externally.

Social networking sites such as Facebook, MySpace and Twitter allow users to publish information about them to be seen by anyone who has access to the site. Generally, these would have limited use in schools but pupils are likely to use these sites at home.

Newsgroups and forums are sites that enable users to discuss issues and share ideas on-line. Some schools may feel that these have an educational value.

Chat rooms are internet sites where users can join in "conversations" on-line;

Instant messaging allows instant communications between two people online. In most cases, pupils will use these at home although school internet systems do host these applications.

Gaming-based sites allow children to "chat" to other gamers during the course of gaming. Many of the gaming sites are not properly moderated and may be targeted by adults who pose a risk to children. Consequently such sites should not be accessible via school internet systems

Social networking sites such as Facebook and access to public/unregulated chat rooms are blocked except for the site hosted by the London Grid for Learning platform, which is used for educational purposes only.

Safety rules

London Grid for Learning hosts an email system that allows pupils to send emails to others within the school or to approved email addresses externally.

- Access to and use of personal email accounts, unregulated public social networking sites, newsgroups or forums, chat rooms or gaming sites on the school internet system is forbidden and may be blocked. This is to protect pupils from receiving unsolicited mail or contacts and to preserve the safety of the system from hacking and viruses.
- If schools identify a clear educational use for emails or social networking sites and forums for on-line publishing, they should only use approved sites such as those provided by the IT service provider. Any use of these sites should be strictly supervised by the responsible teacher.
- Emails should only be sent via the school internet system to addresses within the school system or approved external address. All email messages sent by pupils in connection with school business must be checked and cleared by the responsible teacher.
- Where teachers wish to add an external email address, this must be for a clear educational purpose and must be discussed with the online safety co-ordinator who will liaise with the learning platform provider.
- Apart from the head teacher, individual email addresses for staff or pupils should not be published on the school website.
- Pupils should be taught to be wary of opening attachments to emails where they are unsure of the content or have no knowledge of the sender.
- Pupils should be taught not to disclose personal contact details for themselves or others such as addresses or telephone numbers via email correspondence or on social networking sites.
- All electronic communications should be polite; if a pupil receives an offensive or distressing email or comment, they should be instructed not to reply and to notify the responsible teacher immediately.
- Pupils should be warned that any bullying or harassment via email, chat rooms or social networking sites will not be tolerated and will be dealt with in accordance with the school's anti-bullying policy. This should include any correspondence or contact taking place outside the school and/or using non-school systems or equipment.
- Users should be aware that as use of the school internet system is for the purposes of education or school business only, and its use may be monitored.

Chat rooms, gaming sites and other social networking sites can pose a real risk to children as users can take on an alias rather than their real names and can hide their true identity. The sites may be used by adults who pose as children in order to befriend and gain children's trust (known as "grooming") with a view to sexually abusing them. Children may not be aware of the danger of publishing or disclosing personal information about themselves such as contact details that allow them to be identified or located. They may also inadvertently put other children at risk by posting personal information and photographs without consent.

Newsgroups and forums sites that enable users to discuss issues and share ideas online are not currently used by the school. Should this change -

- Only approved sites such as those provided by the London Grid for Learning platform will be used
- Any use of these sites will be strictly supervised by the responsible teacher

In order to teach pupils to stay safe online outside of school, they should be advised:

- not to give out personal details to anyone on-line that may help to identify or locate them or anyone else, for example home address, name of school or clubs attended
- to only use moderated chat rooms that require registration and are specifically for their age group;
- not to upload personal photos of themselves or others onto sites and to take care regarding what information is posted as there is no control where images may end up or who can see them
- how to set up security and privacy settings on sites or use a "buddy list" to block unwanted communications or deny access to those unknown to them
- to behave responsibly whilst on-line and keep communications polite

- not to respond to any hurtful or distressing messages but to let their parents or carers know so that appropriate action can be taken.
- not to give out personal details to anyone on-line that may help to identify or locate them or anyone else
- not to arrange to meet anyone whom they have only met on-line or go “off-line” with anyone they meet in a chat room
- to behave responsibly whilst on-line and keep communications polite
- not to respond to any hurtful or distressing messages but to let their parents/carers and/or school staff know so that appropriate action can be taken
- To only allow close friends, whom they trust, to have access to their social networking page and set up security and privacy settings or use a “buddy list” to block unwanted communications/deny access to those unknown to them
- That any bullying or harassment via social networking sites, chat rooms or instant messaging will not be tolerated and will be dealt with in accordance with the school’s Anti-bullying Policy

Remote learning platforms:

The Royal Free Hospital children’s school offer remote engagement using the platforms of:

- Google Class room
- Zoom
- Teams (used for professional network meetings)

Livestreaming

Livestreaming is used at the Royal Free hospital children’s school to broadcast an event taking place or to live steam teachers delivering a lesson in a subject specific ‘Google classroom.’ It’s a valuable educational medium which can connect young people, who are unable for various reasons, to not attend school that day.

- Whether hosting or joining a livestream, you must get consent from parents and carers and children if any images of or identifying information about the child may be used. *(See appendix 1 for pupil/parent consent forms)*
- To create a safe environment for children and young people when watching or engaging in a livestream, we have considered the below.

Before starting any livestream, remind children:

- not to share private information
- not to respond to contact requests from people they don’t know
- who they should tell if they see or hear anything upsetting or inappropriate.

School website

- Content cannot be uploaded onto the school website unless it has been authorised by the Headteacher, who is responsible for ensuring that content is accurate, suitable for the purpose and audience, and does not breach copyright or intellectual property law
- Any material to be uploaded onto the website by staff is sent to the Headteacher and/or a designated named person, who will agree it and upload or reject it
- To ensure the privacy and security of staff and pupils, the contact details on the website are the school address, email and telephone number; no contact details for staff or pupils sh9ould be contained on the website
- Children's full names should never be published on the website
- Links to any external websites are regularly reviewed to ensure that their content is appropriate for the school and the intended audience

Photographic and video images

- When the school uses photographs and videos of pupils for publicity purposes, e.g. on the school website, images are carefully selected so that individual pupils cannot be easily identified. It is recommended that group photographs are used
- Where photographs or videos of pupils are used, written permission is first obtained from parents/carers who are informed of the purpose of the image and where it will appear.
- Children's names are never published e.g. on the school website, where their photograph or video is being used
- Staff ensure that children are suitably dressed to reduce the risk of inappropriate use of images
- Images are securely stored only on the school's computer system and all other copies deleted.
- Stored images are not be labelled with the pupil's full name and all images held of children deleted once the child has left the school
- Staff should not use personal devices to take photographs of pupils.
- Schools should inform parents that although they may take photographic images of school events that include other children, it is on the understanding that these images are for personal use only and will not be published on the internet or social networking sites.

Pupils' own mobile phone/handheld systems

The use of mobile phones or other equipment is forbidden during the school day. RFH policy states that no photographs should be taken within the hospital

EXPECTED CONDUCT AND INCIDENT MANAGEMENT

Expected Conduct	In this school, all users: • Are responsible for using the school ICT systems in accordance with the relevant Acceptable Use Policy which they will be expected to sign before being given access to school systems. (at KS1 it would be expected that parents/carers would sign on behalf of the pupils) • Need to understand the importance of misuse or access to inappropriate materials and are aware of the consequences • Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so • Should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's e-safety policy covers their actions out of school, if related to their membership of the school • Will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying Staff • Are responsible for reading the school's e-safety policy and using the school ICT systems accordingly, including the use of mobile phones, and hand held devices Students/Pupils • Should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations Parents/Carers • Should provide consent for pupils to use the internet, as well as other technologies, as part of the e-safety acceptable use agreement form at time of their child's entry to the school • Should know and understand what the 'rules of appropriate use' are and what sanctions result from misuse

Misuse of School technology (devices, systems, networks or platforms)	• Clear and well communicated rules and procedures are essential to govern pupil and adult use of school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school). • These are defined in the relevant Acceptable Use Policy as well as in this document, for example in the sections relating to the professional and personal use of school platforms/networks/clouds, devices and other technology, as well as to BYOD (bring your own device) policy. • Where pupils contravene these rules, the school behaviour policy will be applied; where staff contravene these rules, action will be taken as outlined in the staff code of conduct/handbook It will be necessary to reinforce these as usual at the beginning of any school year but also to remind pupils that **the same applies for any home learning** that may take place in future periods of closure/quarantine etc. Further to these steps, the school reserves the right to withdraw – temporarily or permanently – any or all access to such technology, or the right to bring devices onto school property.
Policy statement	• All incidents and complaints relating to e-safety and unacceptable internet use, whether involving pupils or staff, will be reported to the Headteacher who completes an e-safety incident report form. (See Appendix 5) • A copy of the incident record is emailed to Camden's designated e-safety officer at jenni.spencer@camden.gov.uk. • Where the incident or complaint relates to a member of staff, the matter must always be referred to the Headteacher for action. If the misconduct involves the Headteacher or a governor, the matter should be reported to the Chair of Governors • The Headteacher should keep a log of all e-safety incidents and complaints and regularly review the information for evidence of emerging patterns of individual behaviour or weaknesses in the school's e-safety system, and use these to update the e-safety policy • E-safety incidents involving safeguarding issues, e.g. contact with inappropriate adults, should be reported to the Headteacher or designated Child Protection teacher, who will make a decision as to whether or not to refer the matter to the police and/or Safeguarding and Social Care Although it is intended that e-safety strategies and polices should reduce the risk to pupils whilst online, this cannot completely rule out the possibility that pupils may access unsuitable material on the internet. Neither the school nor the London Borough of Camden can accept liability for material accessed or any consequences of internet access, but all reasonable precautions will be taken to ensure a safe e-learning environment
Unintentional access of inappropriate websites	• If a pupil or staff member accidentally opens a website that has content which is distressing or upsetting or inappropriate to the pupils' age, teachers should immediately (and calmly) close or minimise the screen • Teachers should reassure pupils that they have done nothing wrong and discuss the incident with the class to reinforce the e-safety message and to demonstrate the school's "no blame" approach • The incident should be reported to the Headteacher and details of the website address and URL provided • The Headteacher will liaise with the Schools IT team to ensure that access to the site is blocked and the school's filtering system reviewed to ensure it remains appropriate • It is essential that teachers ensure that where they have asked for filtering to be lifted for a particular lesson (e.g. sex education) that they notify the Schools IT team so that filtering can be put back to minimise the risk of inappropriate sites being accessed by pupils or staff
Intentional access of	• If a pupil deliberately accesses inappropriate or banned websites, they will be in breach of the acceptable use policy and subject to appropriate sanctions (See below)

inappropriate websites by a pupil	• The incident should be reported to the Headteacher and details of the website address and URL recorded • The Headteacher should liaise with the Schools IT team to ensure that access to the site is blocked • The pupil's parents/carers should be notified of the incident and what action will be taken
Inappropriate use of IT by staff	• If a member of staff witnesses misuse of IT by a colleague, they should report this to the Headteacher immediately. If the misconduct involves the Headteacher or governor, the matter should be reported to the Chair of Governors • The Headteacher will remove the computer or laptop and securely store it in order to preserve any evidence. A note of any action taken should be recorded on the e-safety incident report form • The Headteacher will arrange with the Schools IT team to carry out an audit of use to establish which user is responsible and the details of materials accessed • Once the facts are established, the Headteacher will take any necessary disciplinary action against the staff member and report the matter to the school governors and the police where appropriate • If the materials viewed are illegal in nature the Headteacher should report the incident to the police and follow their advice, which should also be recorded on the e-safety incident report form
Online bullying	Online bullying is defined as the use of IT such as email and social media networking sites to deliberately hurt, or upset someone or harass or threaten. Unlike physical forms of bullying, the internet allows bullying to continue past school hours and invades the victim's home life and personal space. It also allows distribution of hurtful comments and material to a wide audience. Online bullying is extremely prevalent as pupils who would not consider bullying in the physical sense may find it easier to bully through the internet, especially if it is thought the bullying may remain anonymous. Bullying may take the form of: • Rude, abusive or threatening messages via email or text • Posting insulting, derogatory or defamatory statements on blogs or social networking sites • Setting up websites that specifically target the victim • Making or sharing derogatory or embarrassing videos of someone via mobile phone or email (e.g. sexting or "happy slapping") Online bullying can affect pupils and staff members. Often, the internet medium used to perpetrate the bullying allows the bully to remain anonymous. In extreme cases, cyber bullying could be a criminal offence under the Harassment Act 1997 or the Telecommunications Act 1984. Materials to support teaching about bullying and useful Department for Education guidance and case studies are at bullying.lgfl.net
Dealing with incidents	The Anti-bullying and behaviour Policy covers cyber bullying and sets out clear expectations of behaviour and sanctions for any breach whether or not they take place on school premises or outside school • Pupils should be told of the "no tolerance" policy for cyber bullying and encouraged to report any incidents to a teacher • Incidents of cyber bullying should be reported to the Headteacher who will record the incident and ensure it is dealt with in line with the school's Anti-bullying Policy. Incidents are monitored and the information used to inform the development of anti-bullying policies • Where incidents are extreme, e.g. threats against someone's life, or continue over a period of time, the matter is reported to the police as in these cases, the bullying may be a criminal offence • Evidence of bullying, e.g. texts, emails or comments on websites should be preserved by the young person as evidence

	• As part of online safety awareness and education, pupils should be told of the "no tolerance" policy for online bullying and encouraged to report any incidents to their teacher.
	• Pupils should be taught:
	  ○ To only give out mobile phone numbers and email addresses to people they trust
	  ○ To only allow close friends whom they trust to have access to their social networking page
	  ○ Not to send or post inappropriate images of themselves
	  ○ Not to respond to offensive messages
	  ○ To report the matter to their parents and teacher immediately.
	• Evidence of bullying, for example texts, emails or comments on websites should be preserved by the young person as evidence.
	Any action taken on online bullying incidents must be proportional to the harm caused. For some cases, it may be more appropriate to help the pupils involved to resolve the issues themselves rather than impose sanctions. This may be facilitated by the School Council or a specialist resource such as Cybermentors.

Action by service providers	All website providers and mobile phone companies have systems in place to deal with problems, such as tracing and blocking communications. Teachers or parents/carers can contact providers for advice on what action can be taken. • Where the bullying takes place by mobile phone texts, the mobile phone company can be contacted to ask them to trace the calls and ensure that any further calls and texts from that number are blocked. The pupil should also consider changing their phone number. • Where the bullying takes place by email, and the messages are being sent from a personal email account, contact the service provider so that the sender can be traced and further emails from the sender blocked. The pupil should also consider changing email address • Where bullying takes place in chat rooms, the pupil should leave the chat room immediately and seek advice from parents/carers or teachers. Bullying should be reported to any chat room moderator to take action • Where bullying involves messages on social networking sites or blogs, contact the website provider to request that the comments are removed. In extreme cases, the bully's access to the site can be blocked • Parents/carers should be notified of any incidents and advised on what measures they can take to block any offensive messages on computers at home
Online bullying of school staff	• Because of the duty of care owed to staff, the Headteacher ensures that school staff are able to report incidents in confidence and receive adequate support, including taking any appropriate action against pupils • The issue of online bullying of school staff is included in discussions with pupils so they aware of their own responsibilities • Incidents involving school staff are recorded and monitored by the Headteacher in the same manner as incidents involving pupils • School staff should follow the guidance in this policy on safe IT use and avoid using their own mobile phones or email addresses to contact parents/carers or pupils so that no record of these details becomes available • Personal contact details for school staff are not posted on the school website or in any other school publication • School staff should follow the advice above on online bullying of pupils and not reply to messages but report the incident to the Headteacher immediately • Where the bullying is being carried out by parents the head teacher should contact the parent to discuss the issue. A home/school agreement with the parent can be used to ensure responsible use.
Sexting and sexual	The internet contains a high level of sexually explicit content and internet-based communications systems and social networking sites can be used to send sexually explicit

abuse and harassment by peers	messages and images. In some cases these actions may be harmful or abusive or may constitute harassment or online bullying. Royal Free Hospital Children's School is aware of the use of IT by older pupils for the purpose of distributing unsuitable materials and sexually harassing other pupils and safeguards pupils from this. "Sexting" or the sending of sexual or intimate photographic images between young people via the internet or mobile devices is a particular issue young people need to know that producing and sharing these images is illegal. Pupils need to understand that once the image is sent, they have lost control of who it is distributed to and how it is used, and that there is a good chance that the image will be widely seen, possibly including parents. Royal Free Hospital Children's School will make a referral to Family Services and Social Work for any pupil who displays sexually abusive behaviour towards other pupils. Staff can also refer to Camden's "Children who harm other children" for further guidance. Staff need to be able to react to incidents in a proportional manner so that the welfare of young people is safeguarded and no young person is unnecessarily criminalised. Guidance for responding to incidents is available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/551575/6.2439_KG_NCA_Sexting_in_Schools_WEB__1_.PDF Schools need to be aware of the use of IT by older pupils for the purpose of distributing unsuitable materials and sexually harassing other pupils and be able to safeguard pupils from this. Schools should be aware of the duty under statutory guidance *Keeping children safe in education* and *Sexual violence and sexual harassment between children in schools and colleges* which requires schools to have policies in place to deal with incidents of on-line sexual harassment. Schools should refer to the CSCB *Sexually harmful behaviour protocol* for further details. https://cscb-new.co.uk/?page_id=8266 Schools should also be aware of when any of these behaviours may be linked to the sexual exploitation of a pupil or is being carried out as a gang- related activity. Staff should refer to the CSCB child sexual exploitation guidance for further details. http://www.cscb-new.co.uk/wp content/uploads/2015/09/Multi_Agency_Guidance_On_Child_Sexual_Exploittion_2015.pdf All schools (regardless of phase) should refer to the UK Council for Internet Safety (UKCIS) guidance on sexting (also referred to as 'youth produced sexual imagery') in schools. NB - where one of the parties is over 18, this is no longer sexting but child sexual abuse. There is a one-page overview called Sexting; how to respond to an incident for all staff (not just classroom-based staff) to read, in recognition of the fact that it is mostly someone other than the designated safeguarding lead (DSL) or online safety lead to first become aware of an incident, and it is vital that the correct steps are taken. Staff other than the DSL must not attempt to view, share or delete the image or ask anyone else to do so, but to go straight to the DSL. The school DSL will in turn use the full guidance document, Sexting in Schools and Colleges to decide next steps and whether other agencies need to be involved It is important that everyone understands that whilst sexting is illegal, pupils/students can come and talk to members of staff if they have made a mistake or had a problem in this area.

Up-skirting	It is important that everyone understands that upskirting (taking a photo of someone under their clothing, not necessarily a skirt) is now a criminal offence, as highlighted in Keeping Children Safe in Education and that pupils/students can come and talk to members of staff if they have made a mistake or had a problem in this area.
Risk from inappropriate contacts and non contact sexual abuse	Teachers may be concerned about a pupil being at risk as a consequence of their contact with an adult they have met over the internet. The pupil may report inappropriate contacts or teachers may suspect that the pupil is being groomed or has arranged to meet with someone they have met on-line. School staff are also aware of pupils being sexually abused on-line through video messaging such as Skype. In these cases, perpetrators persuade the young person concerned to carry out sexual acts while the perpetrator watches/records. • All concerns around inappropriate contacts and potential grooming should be reported to the Headteacher, as designated e-safety contact officer and also the Child Protection Lead • The Headteacher should discuss the matter with the referring teacher and where appropriate, speak to the pupil involved, before deciding whether or not to make a referral to Safeguarding and Social Care and/or the police • The police should always be contacted if there is a concern that the child is at immediate risk, e.g. if they are arranging to meet the adult after school • The Headteacher or Designated Child Protection Lead can seek advice on possible courses of action from Camden's e-safety officer in Family Services and Social Work • Teachers should advise the pupil how to terminate the contact and change contact details where necessary to ensure no further contact • The Headteacher or Designated Child Protection Lead will always notify the pupil's parents/carers of any concerns or incidents and where appropriate, arrange to meet with them discuss what action they can take to ensure their child's safety • Where inappropriate contacts have taken place using school ICT equipment or networks, the Headteacher would note all actions taken and contact the Schools IT team to ensure that all evidence is preserved and that an audit of systems is carried out to ensure that the risk to other pupils is minimised
Risk from contact with violent extremists	Many extremist groups who advocate violence use the internet as a means of either inciting violence against specific groups or providing information on preparing explosives or carrying out terrorist acts. Because of their personal circumstances, some young people may be susceptible to these influences and may be radicalised as a result. All schools have a duty under the Government's Prevent programme to prevent vulnerable young people from being radicalised and drawn into terrorism. The main mechanism for this is Camden's Channel Panel, a multi-agency forum that identifies young people who are at risk and develops a support plan to stop the radicalisation process and divert them from extremism. • Staff are aware of the school's duty under the Prevent programme and are able to recognise any pupil who is being targeted by violent extremists via the internet for the purposes of radicalisation. Pupils and staff are warned of the risks of becoming involved in such groups and informed that accessing such websites is against school policies • The school ensures that adequate filtering is in place and review filtering in response to any incident where a pupil or staff member accesses websites advocating violent extremism. • Pupils and staff should be warned of the risks of becoming involved in such groups and informed that accessing such websites is against school policies • Staff need to be aware of young people who may be more susceptible or are more likely to be targeted or exposed to harmful influences from violent extremists via the internet • All incidents should be dealt with as a breach of the acceptable use policies and the school's behaviour and staff disciplinary procedures will be used as appropriate • The Headteacher will record and review all incidents in order to establish whether there are any patterns of extremist groups targeting the school and whether current school procedures are robust enough to deal with the issue

	• Where there are concerns that a young person is being radicalised or is in contact with violent extremists, or that their parents are and this is placing the child or young person at risk, schools should refer the young person to the Channel Co-ordinator for support.
Risk from sites advocating suicide, self-harm and anorexia	Some internet sites advocate dangerous activities such as self-harming, suicide or anorexia. Other sites contain sexually explicit material or glorify risky and illegal behaviours like substance misuse. Exposure to potentially harmful materials online may normalise the issue for young people and desensitise them to the harm. Most young people who visit these sites will not be adversely affected, but some vulnerable, less resilient young people may feel drawn to the sites which may trigger harmful or even fatal behaviours. • The school ensures that young people have an opportunity to openly discuss issues such as self-harming, suicide, substance misuse and anorexia as part of the PHSE curriculum. • Pastoral support is made available to all young people to discuss issues affecting them and to establish whether their online activities are an added risk factor • Staff receive the training needed to raise awareness of these issues so that they are able to identify those young people who are at risk, offer appropriate support and make appropriate referrals for help.
Social media incidents	See the social media section later in this document for rules and expectations of behaviour for children and adults in the Royal Free school community. These are also governed by school Acceptable Use Policies Breaches will be dealt with in line with the school behaviour policy (for pupils) or code of conduct/handbook (for staff). Further to this, where an incident relates to an inappropriate, upsetting, violent or abusive social media post by a member of Royal Free school community , we will request that the post be deleted and will expect this to be actioned promptly. Where an offending post has been made by a third party, the school may report it to the platform it is hosted on, and may contact the Professionals' Online Safety Helpline (run by the UK Safer Internet Centre) for support or help to accelerate this process.

Risks pupil Wellbeing: • Self-image and identity • Online reputation • Online bullying • Health, wellbeing and lifestyle		
The potential harm or threat	**Description**	**Curriculum area this could be covered in**
Impact on confidence (including body confidence)	Knowing about the impact of comparisons to 'unrealistic' online images. Teaching could include □ exploring the use of image filters and digital enhancement, □ exploring the role of social media influencers, including that they are paid to influence the behaviour (particularly shopping habits) of their followers, □ looking at photo manipulation including discussions about why people do it and how to look out for it.	Health education (secondary) core content – internet safety and harms. "the similarities and differences between the online world and the physical world, including: the impact of unhealthy or obsessive comparison with others online (including through setting unrealistic expectations for body image and how people may curate a specific image of their life online)."
Impact on quality of life, physical and mental health and relationships.	Knowing how to identify when online behaviours stop being fun and begin to create anxiety, including that there needs to be a balance between time spent on and offline. Teaching could include: □ helping pupils to evaluate critically what they are doing online, why they are doing it, and for how long (screen time). This could include reference to technologies that help them to manage their time online, monitoring usage of different apps etc, □ helping pupils to consider quality vs quantity of online activity, □ explaining that pupils need to consider if they are actually enjoying being online or just doing it out of habit, due to peer pressure or the fear of missing out, □ helping pupils to understand that time spent online gives users less time to do other activities. This can lead to some users becoming physically inactive, □ exploring the impact that excessive social media usage can have on levels of anxiety, depression and other	Health Education core content (all stages) – internet safety and harms. "about the benefits of rationing time spent online, the risks of excessive time spent on electronic devices and the impact of positive and negative content online on their own and others' mental and physical wellbeing."

	mental health issues, explaining that isolation and loneliness can affect pupils and that it is very important for pupils to discuss their feeling with an adult and seek support, where to get help.	
Online vs. offline behaviours	People can often behave differently online to how they would act face to face. Teaching could include how and why people can often portray an exaggerated picture of their lives (especially online) and how that can that can lead to perfect/curated lives pressures, discussing how and why people are unkind or hurtful online, when they would not necessarily be unkind to someone face to face.	Relationships Education core content (all stages) – online relationships. “that the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous”
Reputational damage	What users post can affect future career opportunities and relationships – both positively and negatively Teaching could include looking at strategies for positive use, how to build a professional online profile	RSE core content (secondary) – online and media. “about online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online.”
Suicide, self-harm and eating disorders.	Pupils may raise topics including eating disorders, self-harm and suicide. Refer to the Royal Free school self-harm policy. Teachers must be aware of the risks of encouraging or making these seem a more viable option for pupils and should take care to avoid giving instructions or methods and avoid using emotive language, videos or images.	

SANCTIONS FOR MISUSE OF SCHOOL IT

Sanctions for pupils

Sanctions will be applied for breach of acceptable IT use policies reflect the seriousness of the breach and take into account all other relevant factors.

Sanctions for pupils		
Category A	Infringements	Sanctions
Low-level breaches of acceptable use agreements	• Use of non-educational sites during lessons • Unauthorised use of email or mobile phones • Unauthorised use of prohibited sites for instant messaging or social networking	• Referral to the class teacher and/or Headteacher
Category B	Infringements	Sanctions
Persistent breaches of acceptable use agreements following warnings and use of banned sites or serious breaches of e-safety policy that are non-deliberate	• Continued use of non-educational sites during lessons • Continued unauthorised use of email or mobile phones • Continued use of prohibited sites for instant messaging or social networking • Use of file sharing software • Accidentally corrupting or destroying other people's data without notifying staff • Accidentally accessing offensive material without notifying staff	• Referral to class teacher and/or Headteacher • Loss of internet access for a period of time • Contacting parents/carers
Category C	Infringements	Sanctions
Deliberate actions that either negatively affect the London Grid for Learning platform or are serious breaches of acceptable use agreements or Anti-bullying Policy	• Deliberately bypassing security or access • Deliberately corrupting or destroying other people's data or violating other's privacy • Cyber bullying • Deliberately accessing, sending or distributing offensive or pornographic material • Purchasing or ordering items over the internet • Transmission of commercial or advertising material	• Referral to class teacher and/or Headteacher • Loss of internet access for a period of time • Contact with parents/carers • Any sanctions agreed under other school policies
Category D	Infringements	Sanctions
Continued serious breaches of acceptable use agreements following warnings or deliberately accessing and distributing banned or illegal materials which may result in a criminal offence	• Persistent and/or extreme cyber bullying • Deliberately accessing, downloading or disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent • Receipt or transmission of material that infringes the copyright of other people or is in breach of the data protection act • Bringing the school name into disrepute	• Referral to Headteacher • Contact with parents/carers • Possible exclusion • Removal of equipment • Referral to Community police officer and Camden's e-safety officer

Sanctions for staff

These reflect the seriousness with which any breach of acceptable use policies by staff members will be viewed given their position of trust and the need to ensure acceptable standards of behaviour by adults who work with children.

Sanctions for staff		
Category A	Infringements	Sanctions
Minor breaches of the school's acceptable use policy which amount to misconduct and will be dealt with internally by the Headteacher	• Excessive use of internet for personal activities not connected to professional development • Use of personal data storage media (e.g. removable memory sticks) without carrying out virus checks • Any behaviour on the world wide web and social media sites such as Twitter that compromises the staff member's professional standing in the school and community, e.g. inappropriate comments about the school, staff or pupils or inappropriate material published on social networking sites • Sharing or disclosing passwords to others or using other user's passwords • Breaching copyright or licence by installing unlicensed software	• Referral to the Headteacher who will issue a warning
Category B	Infringements	Sanctions
Deliberate actions that undermine safety on the London Grid for Learning platform and activities that call into question the person's suitability to work with children. They represent gross misconduct that would require a strong response and possible referral to other agencies such as the police or Safeguarding and Social Care or Camden's LADO	• Serious misuse of or deliberate damage to any school computer hardware or software, e.g. deleting files, downloading unsuitable applications • Any deliberate attempt to breach data protection or computer security rules, e.g. hacking • Deliberately accessing, downloading or disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent • Receipt or transmission of material that infringes the copyright of other people or is in breach of the data protection act • Bringing the school name into disrepute	• Referral to the Headteacher • Removal of equipment • Referral to Camden's e-safety officer, SSC or police • Suspension pending investigation • Disciplinary action in line with school policies

Date updated: **November 2020**
Date of next review: **November 2023**

Date approved by the Governing Body: 12/11/20

Appendix 1

ACCEPTABLE USE POLICY FOR PRIMARY PUPILS

Name:

I want to stay safe while I am using a computer and I know that anything I do on the computer may be seen by someone else. I will:

- Keep my password secret
- Only open pages which my teacher has said are okay
- Tell my teacher if anything makes me feel scared or uncomfortable
- Make sure all the messages I send are polite
- Tell my teacher if I get a nasty message
- Not reply to any nasty message which makes me feel upset or uncomfortable
- Not give my mobile number, home number or address to anyone who is not a real friend
- Only email people I know or if my teacher agrees
- Only use my school email address
- Talk to my teacher before using anything on the internet
- Not tell people about myself online (I will not tell them my name, anything about where I live or where I go to school)
- Not upload photographs of myself onto the computer
- Never agree to meet a stranger

Parents/carers

□ I have read the above school rules for responsible internet use and agree that my child may have access to the internet through the London Grid for Learning platform. I understand that the school will take all reasonable precautions to ensure pupils do not have access to inappropriate websites, and that the school cannot be held responsible if pupils do access inappropriate websites

□ I agree that my child's work can be published on the school website

□ I agree that photographs that include my child may be published but that any photography will not clearly identify my child and that their name will not be published

Signed: Date:

Appendix 2

ACCEPTABLE USE POLICY FOR SECONDARY PUPILS

Name:

I understand that all computer equipment is owned by the school and that I can use the internet as long as I behave in a responsible way that keeps me and others safe. I also understand that the London Grid for Learning platform is monitored and that if I do not follow the rules, I may not be allowed to use the school computers. I will:

- Only use the school's computers for school work and homework
- Only delete my own files and not look at other people's files without their permission
- Keep my login and password safe and not let anyone else use it or use other people's login or password
- Not bring in files to school without permission
- Ask a member of staff for permission before using the internet
- Not visit websites I know are banned by the school or use non-school email accounts or social networking sites
- Only email people I know or whom my teacher has approved
- Make sure any messages I send or information I upload are polite and sensible
- Not open attachments or download files unless I have permission or I know and trust the person who sent it
- Not give out my home address, phone numbers or send photographs or videos or give any other personal information that may identify me, my family or my friends unless my teacher has given permission
- Never arrange to meet someone I have only met online unless my parent, carer or teacher has given me permission and I will take a responsible adult with me
- Tell my teacher or responsible adult if I see anything I am unhappy with or receive a message I do not like and I will not respond to any bullying messages
- Only use my mobile phone in school when I have permission
- Not use any internet system to send anonymous or bullying messages or to forward chain letters
- Log out when I have finished using the computer

Signed: Date:

Parents/carers

□ I have read the above school rules for responsible internet use and agree that my child may have access to the internet. I understand that the school will take all reasonable precautions to ensure pupils do not have access to inappropriate websites, and that the school cannot be held responsible if pupils do access inappropriate websites

□ I agree that my child's work can be published on the school website

□ I agree that photographs that include my child may be published but that any photography will not clearly identify my child and that their name will not be published

Signed: Date:

Appendix 3

Pupil Digital Rights

We believe that rules and sanctions do not help us become safe users of technology. We agree to abide by our Digital Rights Charter to ensure we have a positive and safe online lifestyle.

- I have the right to enjoy the internet and all the informative, fun and safe things it has to offer within school boundaries and rules.
- I have a right to keep information about myself private. I only have to tell people what I really want them to know in conversation and profiles.
- I have a right to explore the internet but I know that I cannot trust everything that I see or read on the internet and will be discerning in how I use this information.
- I have a right to know who I am talking to on the internet; I don't have to talk to someone if I don't want to.
- I will remember not everyone is who they say they are on the internet. I have a right to tell someone I trust if I think anyone is suspicious.
- I have the right to **not** be videoed or photographed by anyone using cameras, web cams or mobile phones without my permission and for those to not be shared without my permission.
- I have a right **not** to be bullied or intimidated by others through technology (including my phone and social media accounts) and I have the right to report this if this happens.
- I have the right to not be judged by others when I report something that makes me feel uncomfortable or violates my privacy.
- If I accidentally see something I shouldn't, I have the right to tell someone and not to feel guilty or judged about it.
- We are **all** responsible for treating everyone on line with respect. You should not use behaviour or language that would be offensive or upsetting to somebody else.

I have read and understand these rights and agree to follow them when using technology in my education.

Signed: *Date:*

Appendix 4

ACCEPTABLE USE POLICY FOR STAFF AND GOVERNORS

Access and professional use

- All computer networks and systems belong to the school and are made available to staff for educational, professional and administrative purposes only
- Staff and governors are expected to abide by all school online e-safety rules and the terms of this acceptable use policy. Failure to do so may result in disciplinary action being taken
- The school reserves the right to monitor internet activity and examine and delete files from the school's system
- Staff and governors have a responsibility to safeguard pupils in their use of the internet and reporting all e-safety concerns to the e-safety contact officer
- Copyright and intellectual property rights in relation to materials used from the internet must be respected
- E-mails and other written communications must be carefully written and polite in tone and nature
- Anonymous messages and the forwarding of chain letters are not permitted
- Staff should only access approved internet sites via the London Grid for Learning platform. The use of chat rooms and access to personal email accounts or social networking sites and blogs is not allowed during directed time

Data protection and system security

- Staff and governors should ensure that any personal data sent over the internet will be encrypted or sent via secure systems. Where personal data is taken off the school premises via laptops and other mobile systems, the information must be encrypted beforehand
- Use of any portable media such as USB sticks or CD-ROMS is not allowed unless permission has been given by the network manager and a virus check has been carried out
- Downloading executable files or unapproved system utilities will not be allowed and all files held will be regularly checked
- Staff and governors will not allow others to access their individual accounts. Sharing and use of other people's log-ins and passwords is forbidden. Users should ensure that they log-out when they have finished using a computer terminal
- Files should be saved, stored and deleted in line with the school policy
- Care will be taken to check copyright and not publish or distribute others' work without seeking permission.

Personal use

- Staff and governors should not browse, download or send material that could be considered offensive to colleagues and pupils or is illegal
- Staff and governors should not allow school equipment or systems to be used or accessed by unauthorised persons and must keep any computers or hardware used at home safe
- Staff and governors should ensure that personal websites or blogs do not contain material that compromises their professional standing or brings the school's name into disrepute
- School ICT systems may not be used for private purposes without permission from the head teacher.
- Use of school ICT systems for financial gain, gambling, political purposes or advertising is not permitted.

I have read the above policy and agree to abide by its terms.

Name:
Signed: **Date:**

Appendix 5

E-SAFETY INCIDENT REPORT FORM

Name of e-safety contact officer: Alex Yates

Contact details: 0207 472 6298

Details of incident

Date of incident:

Time:

Name of person reporting incident:

If not reported, how was the incident identified?

Where did the incident occur?

□ In school/service setting □ Outside school/service setting

Who was involved in the incident?

□ child/young person □ staff member □ other (please specify)

Type of incident:

□ Bullying or harassment (cyber bullying)
□ Deliberately bypassing security or access
□ Hacking or virus propagation
□ Racist, sexist, homophobic religious hate material
□ Terrorist material
□ Drug/bomb making material
□ Child abuse images
□ Online gambling
□ Soft core pornographic material
□ Illegal hard core pornographic material
□ Other (please specify)

Description of incident

Nature of incident

□ **Deliberate access**

Did the incident involve material being -
□ created □ viewed □ printed □ shown to others □ transmitted to others
□ distributed

Could the incident be considered as –
□ harassment □ grooming □ cyber bullying □ breach of AUP

□ **Accidental access**
Did the incident involve material being -
□ created □ viewed □ printed □ shown to others □ transmitted to others
□ distributed

Action taken

Staff

□ Incident reported to Headteacher/senior manager
□ Advice sought from Safeguarding and Social Care
□ Referral made to Safeguarding and Social Care
□ Incident reported to police
□ Incident reported to Internet Watch Foundation
□ Incident reported to IT
□ Disciplinary action to be taken
□ E-safety policy to be reviewed/amended

Please detail any specific action taken (i.e.: removal of equipment)

Child/young person

□ Incident reported to Headteacher/senior manager
□ Advice sought from Safeguarding and Social Care
□ Referral made to Safeguarding and Social Care
□ Incident reported to police
□ Incident reported to social networking site
□ Incident reported to IT
□ Child's parents/carers informed
□ Disciplinary action to be taken
□ Child/young person debriefed
□ E-safety policy to be reviewed/amended

Outcome of incident/investigation

(This form should be kept on file and a copy emailed to Camden's e-safety officer at jenni.spencer@camden.gov.uk)

Appendix 6:

Reporting a suspicion or disclosure

A pupil may:

- have a bruise, burn or injury that seems suspicious
- show signs of pain or discomfort
- be unnaturally passive or withdrawn
- be unpredictable and challenging
- seem anxious, fearful or distressed
- provide an unlikely explanation for their injury or their behaviour.

Outreach Service

If you have any concerns around:

- feeling unsafe in the working environment
- the late collection of a pupil
- high absconsion risk of a pupil
- feeling threatened at any time

Follow the RFHCS safeguarding procedures

Suspicion or disclosure that a pupil is at risk of harm

↓

Is emergency treatment needed?

No → If there is an urgent safety issue, find the designated safeguarding lead or deputy head teacher immediately

Yes → Arrange medical help and inform the designated safeguarding lead that it is a child protection issue

If a pupil discloses to you, listen and reassure. Let them know you need to pass on the information. Tell them what will happen next.

If you have a suspicion but the pupil has not disclosed

Notify the designated safeguarding lead of your action as soon as possible

↓

Complete the record of concern before the end of the day

↓

Hand the record of concern to the designated safeguarding lead before the end of the same day

↓

Maintain confidentiality. Do not contact parents.
The designated person will advise how parents will be contacted and who else needs to know

Designated Safeguarding Lead - Jemma Michelson

In absence of Designated Safeguarding Lead inform Alex Yates (Head)

Camden Social Work Team 020 7974 4094	RFHCS Safeguarding Governor Diana Goldin 020 7794 0500	Royal Free Hospital Trust Safeguarding Lead –Helen Swarbrick Pager - 1616

Appendix 6

DESCRIPTION OF ICT APPLICATIONS

Technology/ Application	Description/Usage	Benefits	Risks
Internet	• Enables the storage, publication and retrieval of a vast range of information • Supports communications systems	• Provides access to a wide range of educational materials, information and resources to support learning • Enables pupils and staff to communicate widely with others • Enhances schools management information and business administration systems	• Information is predominantly for an adult audience and may be unsuitable for children • The vast array of information makes retrieval difficult without good research skills and ability to critically evaluate information • Access to sites promoting illegal or anti-social activities, extreme views or commercial and gambling sites
Email	• Allows written communications over the network and the ability to attach documents	• Enables exchange of information and ideas and supports collaborative working • Enhances written communications skills • A good form of communication for children with some disabilities	• Difficulties controlling contacts and content • Use as a platform for bullying and harassment • Risks from unwanted spam mail, particularly for fraudulent purposes or to introduce viruses to systems • Hacking • Unsolicited mail
Chat/instant messaging	• Chat rooms allow users to chat online in real time in virtual meeting places with a number of people • Instant messaging allows real-time chat for 2 people privately with no-one else able to join. Users have control over who they contact through "buddy lists"	• Enhances social development by allowing children to exchange experiences and ideas and form friendships with peers • Use of pseudonyms protects the child's identity • Moderated chat rooms can offer some protection to children	• Anonymity means that children are not aware of who they are really talking to • Chat rooms may be used by predatory adults to contact, groom and abuse children online • Risk of children giving away personal information that may identify or locate them • May be used as a platform to bully or harass
Social networking sites	• Online communities, including blogs and podcasts, where users can share text, photos and music with others by posting items onto the site and through messaging • It allows creation of individual profiles • Users can develop friends lists to allow access to individual profiles and invite comment	• Allows children to network with peers and join forums to exchange ideas and resources • It provides a creative outlet and improves ICT skills	• Open access means children are at risk of unsuitable contact • Risk of children posting unsuitable material online that may be manipulated to cause them embarrassment or distress • Children may post personal information that allows them to be contacted or located • May be used as a platform to bully or harass
File sharing (peer-to-peer networking)	• Allows users to share computer capability, networks and file storage • Used to share music, video and other materials	• Allows children to network within a community of peers with similar interests and exchange materials	• Illegal download and copyright infringement • Exposure to unsuitable or illegal materials • Computers are vulnerable to viruses and hacking
Mobile phones & multi-media equipment	• Mobile phones now carry other functions such as cameras, video-messaging and access to internet and email	• Provide children with a good means of communication and entertainment • They can also keep children safe and allow them to be contacted or stay in contact	• Their mobile nature makes supervision of use difficult leading to risks of unsuitable contacts or exposure to unsuitable material on the internet or through messaging • Risk from violent crime due to theft • Risk of online bullying via mobile phones

Appendix 7:

Young Person's & Parent/Carer agreement:

Please observe the following rules when using Zoom/Google classroom:

Safeguarding- please keep yourself and others safe whilst using Zoom/ Google Class room for online learning.

In the event that you have any concerns about inappropriate use online during these sessions, please do not hesitate to contact the Royal Free Linked-up course leader Mike Kelly, your child's teacher and/or personal Tutor with any safeguarding concerns.

- Under NO circumstance should you film, screenshot or record the Zoom/Google Class room session of each other, or of teaching staff with the intention to share it with anyone.
  - **When learning is taking place on this online platform, a Parent/Carer/teaching professional to be present and observing in the room throughout the session to ensure safeguarding practices are being followed.**
  - Zoom/Google Class room is a platform to engage you in learning during this time- if this platform is not used in a responsible way, the consequences could be serious.
  - If you have any questions or concerns, please contact your teacher, personal tutor and they can give you further advice.

Be sensible and respectful of others during Zoom/Google class room lessons.

- Remember to use appropriate language when online just like you would if you were in a lesson at school.

Keep focused only on the learning during the Zoom/Google class room sessions.

- Yes- we understand that this is a different way to be 'in class' together but remember- these sessions are for learning- we ask that you do not use this platform as a place to socialise with your peers.

When the lesson has begun- try to speak one person at a time

- There are emoji tools in Zoom /Google class room which identify who in the room would like to make a comment or ask a question.
- Raise your hand to the camera OR use the emoji tools of a hand to show that you want to say something.
- In Google class room, you can make a shared comment to the group in the comments box.
- When you are not speaking, we ask that you mute your microphone.

If you do not want to show your face on the screen you can switch the video option off to select only the audio features

- You may not feel like showing your face; this is fine.
- It is very easy to turn your camera off and still engage in the lesson.
- With the camera off, you can still be heard with your audio and we would like you to make verbal contributions to the session.

Ensure that you are sitting in a place in your home, which has good lighting and (if possible) at a table.

- We realise that everyone has a different living situation, but ask that if you can, try and be in a place where you will not be distracted by your surroundings, is quiet and others would not be visible on screen.

Remember to dress appropriately during the Zoom/Google class room session.

- We would not expect you to dress in school uniform! However, we ask that you dress appropriately on the screen.
- If you are unsure what this may include, please refer to your parent/carer, teacher or personal tutor for specific guidance.

An adult should be present during the Zoom/Google class room teaching session.

- When learning is taking place on this online platform, a Parent/Carer/teaching professional to be present and observing in the room throughout the session to ensure safeguarding practices are being followed.

Your mobile phone or any other tablet device should be switched off during the Zoom /Google class room lesson so there are no interruptions.

- Just like during a 'normal' lesson in your school, you we ask that you do not access to your mobile during lessons to text, call or use for any other purpose.
- We ask that you turn you phone off during the session.

Sharing a love of learning
ROYAL FREE
HOSPITAL CHILDREN'S SCHOOL

Dear Parents/carers/referring professionals,

Please read and discuss this agreement below for using remote access teaching via Zoom/Google Class room with your child. We ask that you then respond via email to consent to engaging in Zoom/ Google classroom lessons with RF teachers and other professionals working with Royal Free school to say:

Parents/carers/referring professionals:

We have discussed this online safety agreement with (Young person's name here) and they have agreed to follow the rules set out below in line with the Royal Free Hospital Children's school IT and Safeguarding policy.

I (parent/carers name here), consent to my child taking part in the stated activity: Zoom/Google class room online E-learning lessons from teachers and/or other professionals working at the Royal Free Hospital Children's School.

When learning is taking place on this online platform, I agree to be present and observing in the room to ensure safeguarding practises are being followed.

Young person:

I (Young persons' name here) understand that engaging, enjoying the learning activity and being safe means I need to follow the behaviour code and safety rules as expected at the Royal Free Hospital Children's school.

The school email to reply to is the admin account: admin@royalfree.camden.sch.uk

If you have any further questions or concerns, please contact: michael.kelly@royalfree.camden.sch.uk Linked up Coordinator

Appendix 8:

Sharing a love of learning
ROYAL FREE
HOSPITAL CHILDREN'S SCHOOL

Risk Assessment for Zoom

(To completed by Personal Tutor/Teacher or Key professional known to the young person)

Surname	**DoB:**
First name	**Local Authority** : Camden
First language	**Date of PLAN:**

*** Current SUPPORTING AGENCIES/PROFESSIONALs *(CAMHS/EP/SALT/CP/LAC)***	
NAME/ROLE	**CONTACT DETAILS**

*** Historically Known RISK BEHAVIOUR**	**Yes/NO**	**E-learning Risk behaviour for (ZOOM/ Google class room)**	**Yes/NO**
Suicidal ideation or severe harm		**Consider the potential risks when your tutee is engaging in Zoom/ google class room Learning.** **Are they at risk of displaying the following behaviour?**	
Violence to others		**Sexualised behaviour on camera**	
Severe self neglect		**Use inappropriate language /phrases which could 'trigger' or upset others**	
Risk from others (e.g. exploitation)		**Unable to cope with the full length of the Zoom/google class room lesson due to medical or special educational need (**	

		Consider making the lessons shorter to support this need)	
Risk to intellectual/social development		**Is the young person in a living space which can accommodate Zoom/ google class room learning and will safeguard themselves and others in the home?**	
Sexualised behaviour		**Dressing appropriately whilst on Camera**	
Uses inappropriate language		**Adhere to any of the RFHCS behavioural expectations when engaging in a Zoom/ google class room lesson as stated in the guidance given in the school Google class room drive as well as signed contract by parents and pupils.**	
History of Self- Harm		**Have the parents and young person signed the RFHCS consent form for engaging in Zoom/ google class room E-learning lessons?**	
Online exploitation			
Unable to keep safe online (social media/other online platforms)			

***Additional comments by personal tutor/teacher or Key professional known to the young person**
Early warning signs, relapse indicators, triggers

ACTIONS/INTERVENTIONS TO MEET IDENTIFIED NEEDS/MANAGE RISK **ACTION TO BE TAKEN IN THE EVENT OF A CRISIS**
Agreed school response to a crisis and who to contact
• In the event that a young person displays behaviour which is inappropriate or a cause for concern- personal tutor will document this following the RF safeguarding procedures and Alert safeguarding Leads (AY/JM) at the RFHCS to ensure that if the young person needs further support to keep themselves safe online – this can be offered. • If Risk is shown using Zoom online, personal tutor will contact the young person and their parents/home school directly and discuss any use of behaviours, which show a concern as mentioned above. • Inform external/internal professionals of this 'Risk' behaviour if necessary. In includes also updates about progress and positive engagement online • If inappropriate use of Zoom by a young person is identified in the 'group' lessons- consider the alternative in arranging an individualised timetable in which 2:1 learning takes place instead during the 'open' spaces of the Online RF school timetable

Signed by Personal Tutor:_____

Date:_____