RICHMOND HOUSE SCHOOL
Where children are happy to learn

Online Safety Policy		Associated Policies
Last reviewed	January 2025	Safeguarding and Child Protection
Next review	**January 2028**	Anti-bullying Policy
Gov. sub-committee	Education	Behaviour Policy
Owner	Designated Safeguarding Lead	Staff Code of Conduct
Online Safety Co-ordinator		Data Protection Procedure
		Privacy Notice
		Records Retention Procedure
		Health and Safety Policy
		Taking, Storing and Using Images of Children Policy
Network Manager:	*Bursar*	PSHE and Computing Curriculum
		Acceptable Use Agreements

Richmond House School fosters a dynamic learning environment by offering a range of ICT opportunities and tools. This empowers students to make informed and safe choices, supporting their personalised learning journeys in alignment with the school's vision.

Introduction

It is the duty of Richmond House School to ensure that every pupil in its care is safe and the same principles apply to the digital world as apply to the real world. IT and online communications provide unrivalled opportunities for enhanced learning in addition to traditional methods but also pose greater and more subtle risks to young people. Pupils are therefore taught how to stay safe in the online environment and how to mitigate risks, including but not limited to the risk of identity theft, bullying, harassment, grooming, stalking, abuse, radicalisation and online persona. Technology is continually enhancing communication, the sharing of information, learning, social interaction and leisure activities. However, many information technologies, particularly online resources, are not effectively policed. All users need to be aware, in an age-appropriate way, of the range of risks associated with the use of these internet technologies. Current and emerging technologies used in and outside of school include:

· Websites;

· Email and instant messaging;

· Blogs, forums and chat rooms;

· Mobile internet devices such as smart phones and tablets;

· Social networking sites;

· Music / video downloads;

· Gaming sites and online communities formed via games consoles;

· Instant messaging technology via SMS or social media sites;

· Video calls;

· Podcasting and mobile applications;

· Virtual and augmented reality technology; and

· Artificial intelligence

This policy, supported by the Acceptable Use Agreements (for staff, visitors and pupils), is implemented to protect the interests and safety of the whole school community. It aims to provide clear guidance on how to minimise risks and how to deal with any infringements.

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

Richmond House School understands the responsibility to educate pupils about online safety issues; teaching them the appropriate behaviours and critical thinking skills necessary to enable them to remain both safe and within the law when using the internet and related technologies in and beyond the classroom. The School also understands the importance of involving pupils in discussions about online safety so they can share their thoughts and ideas, to ask questions and speak out if they have felt endangered.

Scope of this Policy

This policy applies to all members of the school community, including staff, pupils, parents and visitors, who have access to and are users of the school IT systems. 'Visitors' are deemed as anyone else who comes to the School that are not teaching or non-teaching staff including supply teachers, student teachers and occasional volunteers.

Both this policy and the Acceptable Use Agreements (for all staff, visitors and pupils) cover both fixed and mobile internet devices provided by the School (such as PCs, laptops, webcams, tablets, whiteboards, digital video equipment, etc.); as well as all devices owned by pupils, staff, or visitors and brought onto school premises (personal laptops, tablets, smart phones, smart watches etc.).

Roles and Responsibilities

1. The Governing Body

The Governing Body of the School, through the Education Sub-Committee, is responsible for the approval of this policy and for reviewing its effectiveness.

2. Headteacher and the Senior Leadership Team

The Headteacher is responsible for the safety of the members of the school community, and this includes responsibility for online safety. The Headteacher has delegated day-to-day responsibility to the Online Safety Co-Ordinator and the Deputy Head, who is the DSL.

In particular, the role of the Headteacher and the Senior Leadership team is to ensure that:

- staff, in particular the DSL, DDSLs and the Online Safety Co-Ordinator, are adequately trained
- staff are aware of the school procedures and policies that should be followed in the event of abuse or suspected breach of online safety in connection to the school.

3. The DSL, DDSL and Online Safety Co-ordinator

The School's DSL is responsible to the Headteacher for day-to-day issues relating to online safety. The Online Safety Coordinator will work with the DSL and the school's Network Manager, the Bursar, and IT support team to ensure this policy is upheld by all members of the school community. They will keep up to date on current online safety issues and guidance issued by relevant organisations, including the ISI, the Local Authority, CEOP (Child Exploitation and Online Protection), Childnet International and the Local Authority Safeguarding Children Board.

They will monitor the Filtering and Monitoring system alerts and follow up any concerns in a timely manner using the information given. Any inappropriate usage of the school's computing system will be investigated by the Pastoral Team and dealt with in line with the school's Behaviour Policy. This will be recorded on children's individual records as necessary.

4. Network Manager – The Bursar

The school's Network Manager is responsible for maintaining a safe technical infrastructure at the school. They will work with advice from the IT support team to keep abreast with the rapid succession of technical developments, to ensure the security of the school's hardware system and its data, and for training the school's teaching and administrative staff in the use of IT. The Network manager with support from the IT support team will maintain the filtering system. Any inappropriate usage by staff will be dealt with in line with the school's Disciplinary Procedure.

5. Teaching and Support Staff

All staff are required to read the school's Online Safety Policy and the Staff Code of Conduct and sign the Staff Acceptable Use Agreement before accessing the school's systems.

As with all issues of safety at this school, staff are encouraged to create a talking and listening culture to address any online safety issues which may arise in classrooms daily.

Staff must report any suspected misuse or problem to the Online Safety Co-ordinator and the DSL.

6. Pupils

Pupils are responsible for using the school IT systems in accordance with the Acceptable Use Agreement, and for letting staff know if they see IT systems being misused or if our Filter and Monitoring system has appeared on their screen. Given the nature of our Filtering and Monitoring system, this could be for innocuous reasons but as part of safe practice, pupils must make the teacher aware when it happens. This will allow for the Online Safety Coordinator and the pastoral team to quickly resolve any issues.

The Acceptable Use Agreements vary between Phase 1 and Phase 2 and can be found in Appendix 1 and Appendix 2. Copies of the agreement are stored in a central location for staff to share and use with their classes. Phase 1 classes are expected to discuss and sign a class copy of their Acceptable Use Agreement, whereas Phase 2 classes are expected to discuss their agreements and sign them individually.

7. Parents and Carers

Richmond House School believes that it is essential for parents to be fully involved with promoting online safety both in and outside of school. The School regularly consults and discusses online safety with parents and seeks to promote a wide understanding of the benefits and risks related to internet usage. Our Wednesday Wise Up is designed to keep parents updated and informed on a wide range of school related information, including online safety. The school will always contact parents if it has any concerns about pupils' behaviour in this area and likewise it hopes that parents will feel able to share any concerns with the school.

Education and Training

1. Staff: Awareness and Training

New staff receive information on Richmond House School's Online Safety and Acceptable Use Agreement as part of their induction.

All staff receive regular information and training on online safety issues, including Prevent training, in the form of INSET training, internal meeting time, and regular cyber security training. All teachers are made aware of their individual responsibilities relating to the safeguarding of children within the context of online safety. Any visitors using the school's IT resources should read the Online Safety Policy and sign the Acceptable Use Agreement.

All teachers working with children are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following school Online Safety procedures. These behaviours are summarised in the Acceptable Use Agreement which must be signed and returned before using any technology in school. When children use school computers, staff should make sure children are fully aware of the agreement they are making to follow the school's IT guidelines.

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

If children are being asked to learn online at home, the School will refer to Section 11 of the Safeguarding Policy titled 'Remote Learning and Remote Welfare'. This states that schools should follow advice from the DfE on Safeguarding and Remote Education (DfE, 2021b) and follow the Guidance for Safer Working Practice (Safer Recruitment Consortium, 2019)

2. Pupils: Online safety in the Curriculum

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

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

Pupils should be aware of the impact of cyber-bullying and know how to seek help if they are affected by these issues (see also the school's Anti-bullying Policy, which describes the preventative measures and the procedures that will be followed when the school discovers cases of bullying). Pupils should approach the Pastoral team as well as parents, peers and other school staff for advice or help if they experience problems when using the internet and related technologies.

Richmond House School plans Computing lessons to cover Online Safety and the 4 Cs of online risk in the first half term of every academic year. These are summarised below (Safer Internet Website 2021) See https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues for further details. This gives our pupils the best chance to be up to date on the latest guidance and to be prepared for their online activity in the year ahead.

Conduct: *children may be at risk because of their own behaviour, for example, by sharing too much information*

Children need to be aware of the impact that their online activity can have on both them and other people, and the digital footprint that they create on the internet. It's easy to feel anonymous online and it's important that children are aware of who can view, and potentially share, the information that they may have posted. When using the internet, it's important to keep personal information safe and not share it with strangers. Discuss with children the importance of reporting inappropriate conversations, messages, images and behaviours and how this can be done. This extends to discussions about the consensual and non-consensual sharing of nude and semi-nude images and/or videos.

Content: *age-inappropriate or unreliable content can be available to children*

Some online content is not suitable for children and may be hurtful or harmful. This is true for content accessed and viewed via social networks, online games, blogs and websites. It's important for children to consider the reliability of online material and be aware that it might not be true or written with a bias. Children may need help as they begin to assess content in this way. There can be legal consequences for using or downloading copyrighted content, without seeking the author's permission.

Contact: *children can be contacted by bullies or people who groom or seek to abuse them*

It is important for children to realise that new friends made online may not be who they say they are and that once a friend is added to an online account, you may be sharing your personal information with them. Regularly reviewing friends lists and removing unwanted contacts is a useful step. Privacy settings online may also allow you to customise the information that each friend is able to access. Children will be taught to identify the signs of cyberbullying and what actions they can take if they become a victim. This could be child on child abuse from known contacts or inappropriate contact from others online. If a child is the victim of cyberbullying, this can be reported online, via the Report Abuse button on most websites (which the children will be shown) or by contacting the site/app directly. Children should be encouraged to report any online bullying, directed towards themselves or others, to a trusted adult. Staff should also report any concerns about cyberbullying to the Pastoral Team. If the perpetrator is a member of the school`s pupil body, the behaviour and anti-bullying policies will be followed to decide on the appropriate course of action. If they are not from Richmond House School, the online safety co-ordinator will take action to prevent this continuing which could include contacting the website/app provider or contacting the police. Staff should be aware that Child Sexual Exploitation (CSE) is a form of child sexual abuse and may include noncontact activities via the internet. If a member of staff has concerns that a child is, or has been, the subject of inappropriate sexual contact or approach by another person, it's vital that they report it to the DSL who will contact the police via the Child Exploitation and Online Protection Centre (**www.ceop.police.uk).** Staff will reinforce with children the importance of telling a trusted adult straight away if someone is bullying them or making them feel uncomfortable online, or if one of their friends is being bullied online.

Commercialism: *young people can be unaware of hidden costs and advertising in apps, games and websites*

Young people's privacy and enjoyment online can sometimes be affected by advertising and marketing schemes, which can also mean inadvertently spending money online, for example within applications. Staff will encourage children to keep their personal information private, learn how to block both pop ups and spam emails, turn off in-app purchasing on devices where possible, and use a family email address when filling in online forms.

3. Parents

The school seeks to work closely with parents and guardians in promoting a culture of online safety. The school will always contact parents if it has any concerns about pupils' behaviour in this area and likewise it hopes that parents will feel able to share any concerns with the school.

The school recognises that not all parents and guardians may feel equipped to protect their child when they use electronic equipment at home. The school therefore will offer advice about online safety and the practical steps that parents can take to minimise the potential dangers without curbing their natural enthusiasm and curiosity.

Regular Safeguarding updates and filtering and monitoring advice is given to parents and carers through our usual communication means. Policies relating to Online Safety and Safeguarding are made available on our school website and any publications or guidance that we feel is pertinent to share with parents is done so via our Wednesday Wise up.

Policy Statements

1. Use of School and Personal Devices

Staff

School devices assigned to a member of staff as part of their role must have a password (which should be changed regularly) or device lock, so that unauthorised people cannot access the content. When they are not using a device staff must ensure that it is locked to prevent unauthorised access.

Staff at Richmond House School are permitted to bring in personal devices for their own use; however, staff are not allowed to use their personal devices while with children (except in emergencies) or at any time within the Early Years setting. They may **only** use such devices during break-times, lunchtimes, non-contact lessons or before/after the school day.

Under no circumstances may staff contact a pupil using a personal telephone number, email address, social media, or other messaging system.

Personal telephone numbers, email addresses, or other contact details should not be shared with parents for anything related to school business, unless in an emergency, with permission from the Headteacher or DSL.

Pupils

Pupils must not bring mobile devices into school, unless they have been given permission by the Headteacher (e.g. for use during the journey to and from school). They must be handed in to the school office at the start of the day and collected as they leave school. These requirements apply to phones and all devices that communicate over the internet, including smartwatches and other wearable technology.

The School recognises that mobile devices are sometimes used by pupils for medical purposes or as an adjustment to assist pupils who have disabilities or special educational needs. Where a pupil needs to use

a mobile device for such purposes, the pupil's parents or carers should arrange a meeting with the Headteacher or SEND Lead to agree how the school can appropriately support such use. The Headteacher will then inform the pupil's teachers and other relevant members of staff about how the pupil will use the device at school.

2. Use of Internet and email

Staff

Staff must not access social networking sites or any website or personal email which is unconnected with school work whilst with pupils. Such access may only be made during breaktimes, lunchtimes, non-contact lessons or before/after the school day, and only on personal devices.

Staff must use social networking sites with extreme caution, being aware of the nature of what is published online and its potential impact on their professional position and the reputation of the school.

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

Staff must immediately report to the DSL the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication. Staff must remain alert to the risk of fraudulent emails and should report emails they suspect to be fraudulent to the Network Manager.

Any online communications must not either knowingly or recklessly:

- place a child or young person at risk of harm, or cause actual harm;
- bring Richmond House School into disrepute;
- breach confidentiality;
- breach data protection legislation;
- or do anything that could be considered discriminatory against, or bullying, or harassment, of any individual in the school.

Under no circumstances should school pupils be added as social network 'friends' or contacted through social media or personal email by any member of staff.

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

The Professionals Online Safety Helpline is available to help teachers with any online safety issues, including any affected by the increase in explicit, offensive and harmful videos about teachers on social media, especially Tik Tok. The Professionals Online Safety Helpline can be contacted on: 0344 381 4772 and helpline@saferinternet.org.uk. Advice on dealing with these issues can be found on the UK Safer Internet Centre website.

Pupils

There is strong anti-virus and firewall protection on the School network. Spam emails and certain attachments will be blocked automatically by the email system. If this causes problems for school work / research purposes, pupils report this to their teacher who should contact the Network Manager for assistance.

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

The School expects pupils to think carefully before they post any information online, or repost or endorse content created by other people. Content posted should not be able to be deemed inappropriate or offensive, or likely to cause embarrassment to the individual or others.

Pupils must report any accidental access to materials of a violent or sexual nature to a member of staff who must log the incident in writing to the DSL and Network Manager. Deliberate access to any inappropriate materials by a pupil will lead to the incident being recorded on their file and will be dealt with under the school's Behaviour Management Policy. Pupils should be aware that all internet usage via the school's systems and its Wi-Fi network is monitored.

The PSHE and Computing curriculum includes advice on what constitutes appropriate and inappropriate use of the internet.

If an individual child is considered to need additional help to keep themselves and others safe when using the internet, they may be referred to InCtrl. This is a program that aims to increase safe online behaviours and the digital resilience of children aged 9–13. See Appendix 7 for further details.

3. Data Storage and Processing

The school takes its compliance with the Data Protection Act 2018 seriously. Please refer to the Data Protection Procedure, Privacy Notice Policy, Records Retention Procedure and the Acceptable Use Agreements for further details.

Pupils are expected to save all data relating to their work on the school network. Staff are expected to save all data relating to their work to their school laptop/ PC, to the school's central server or to OneDrive. Staff must not save work to the hard drives on these devices and take them from the building unless they are encrypted. Staff should be aware that information stored on the hard drive is not backed up and therefore could be lost in the event of a computer failure.

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

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

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

4. Password Security

Pupils have storage folders on the server, which are used from Year 2 upwards.

Children in Reception are given their own login to the school network in the Summer Term to help with their transition to Year One. Pupils in Reception to Year Four will have a generic, class password that will allow them onto the school system. Pupils in Years Five and Six will be allowed to have personalised passwords. However computing teachers will keep a secure, central record of these so access for staff would be easy if required.

Staff should ensure they use strong, unique passwords (usually containing eight letters or more, and containing upper and lower case letters as well as numbers), which should be changed if there is any risk

to security. Multi Factor Authentication will be employed for access to the school network when working remotely.

In Office 365, the “stay signed in” option must only be used when accessing via a secure device which is password protected and used only by one user. If accessing Office 365 via a device without secure password protection, or on a shared device, the “stay signed in” option must not be used.

5. Safe use of Digital and Video Images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying, stalking or grooming to take place.

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

Parents / carers may take videos and digital images of their children at school events for their own personal use, in accordance with the Taking, Storing and Using Images of Children Policy. To respect everyone's privacy, and in some cases protection, these images should not be published on blogs or social networking sites (etc.) without the permission of the people identifiable in them (or the permission of their parents), nor should parents comment on any activities involving other pupils in the digital / video images.

Staff and volunteers are allowed to take digital / video images to support educational aims on school equipment, but must follow school policies regarding the sharing, distribution and publication of these images. These images should only be taken on school equipment; personal equipment should not be used for such purposes.

The School adheres to the following checklist when publishing images of pupils:

- ensure students are dressed appropriately. At sports events for example, the School will not publish pictures of pupils in swimming costumes
- ensure electronic images are stored confidentially and securely and are accessed only by staff with authority to do so
- never show, copy, or give an image to any unauthorised person
- avoid using the last name of a pupil and will always ensure that parents have consented to use of images before publishing the image

Pupils must not take, use, share, publish or distribute images of others.

School handles the images according to its obligations under the Data Protection Act 2018.

6. Misuse

Richmond House School will not tolerate illegal activities or activities that are inappropriate in a school context, and will report illegal activity to the Police and/or the LSCP. If the school discovers that a child or young person is at risk as a consequence of online activity, it may seek assistance from CEOP.

Internet Use will be monitored, both on school devices and on devices using the school wifi. Any misuse identified by our filtering service will be investigated by the DSL, DDSL and/or Internet Safety Lead. Incidents of misuse or suspected misuse must be dealt with by the DSL in accordance with the school's policies and procedures, in particular the Safeguarding Policy.

The school will impose a range of sanctions on any pupil who misuses technology to bully, harass or abuse another pupil in the school in line with the Anti-Bullying and Behaviour Policies.

Signed (Headteacher)

Signed (Chair of Governors)

Appendix 1

Richmond House School - Acceptable Use Agreement (Phase 2)

Introduction

Digital technologies have become integral to the lives of children and young people, both within and outside schools. These technologies are powerful tools, which open up new opportunities for everyone. They can stimulate discussion, encourage creativity, and stimulate awareness of context to promote effective learning. Learners should have an entitlement to safe access to these digital technologies.

This acceptable use agreement is intended:

- to ensure that learners will have good access to devices and online content, be responsible users and stay safe while using digital technologies for educational, personal and recreational use
- to help learners understand good online behaviours that they can use in school, but also outside school
- to protect school devices and networks from accidental or deliberate misuse that could put the security of the systems and users at risk.

Acceptable Use Agreement

When I use devices, I must behave responsibly to help keep me and other users safe online and to look after the devices.

- I understand that what I do online will be supervised and monitored and that I may not be allowed to use devices in school unless I follow these rules and use them responsibly.
- I will only visit internet sites that adults have told me are safe to visit.
- I will keep my username and password safe and secure and not share it with anyone else.
- I will be aware of "stranger danger" when I am online.
- I will not share personal information about myself or others when online.
- I will immediately tell an adult if I see anything that makes me feel uncomfortable when I see it online.

I will look after the devices I use, so that the school and everyone there can be safe:

- I will handle all the devices carefully and only use them if I have permission.
- I will not try to alter the settings on any devices or try to install any software or programmes.
- I will tell an adult if a device is damaged or if anything else goes wrong.
- I will only use the devices to do things that I am allowed to do.

I will think about how my behaviour online might affect other people:

- When online, I will act as I expect others to act toward me.
- I will not copy anyone else's work or files without their permission.
- I will be polite and responsible when I communicate with others, and I appreciate that others may have different opinions to me.
- I will not take or share images of anyone without their permission.

I know that there are other rules that I need to follow:

- I will only bring my personal device to school if I need it to walk to or from school and I know I will leave it in the office throughout the day.

- I will not use any social media sites in school.
- Where work is protected by copyright, I will not try to download copies (including music and videos).
- When I am using the internet to find information, I should take care to check that the information is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.
- I should have permission if I use the original work of others in my own work.

I understand that I am responsible for my actions, both in and out of school:

- I know that I am expected to follow these rules in school and that I should behave in the same way when out of school as well.
- I understand that if I do not follow these rules, I may be subject to disciplinary action. This could include loss of use of computer systems in school, contacting of parents/carers and in the event of illegal activities involvement of the police.
-

Learner Acceptable Use Agreement Form

As a pupil at Richmond House School, I agree to follow these guidelines when:

- I use the school systems and devices (both in and out of school)
- I am out of school and involved in any online behaviour that might affect the school or other members of the school.

Name of Learner: Group/Class:

Signed: Date:

Appendix 2

Richmond House School - Acceptable Use Agreement (EYFS/Phase 1)

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers/tablets.
- I will only use activities that a teacher or suitable adult has told or allowed me to use.
- I will take care of computers/tablets and other equipment.
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong.
- I will tell a teacher or suitable adult if I see something that upsets me on the screen.
- I know that if I break the rules, I might not be allowed to use a computer/tablet.

Signed (class and class teacher):

Date: September 2024

Appendix 3

STAFF AND ANYONE GIVEN ACCESS TO THE SCHOOL NETWORK

ACCEPTABLE USE AGREEMENT

I confirm that I have read and understood the online safety policy and the staff code of conduct and I will use all means of electronic equipment provided by the school and any personal devices which I use for school activity in accordance with this policy and the staff code of conduct.

Terms of Agreement

I understand that I must use school systems in a responsible way to ensure that there is no risk to my professional or personal online safety or the online safety and security of the systems and other users.

- Any online communications or any communications sent from a school email address will be professional and respectful of others and maintain the reputation of the school.
- Online, live stream lessons should be conducted as a group and all individual lessons should have another adult present or be recorded for your protection.
- To protect my own privacy, I will only use a school email address and school phone numbers (including school mobile phones) as contact details for children and their parents, unless in a case of emergency.
- I will not share any personal telephone numbers, email accounts or social media accounts with pupils.
- I will not communicate with parents using personal phone numbers, email accounts or social media accounts on matters of school business.
- I shall only communicate with parents about matters relevant to School life using official School systems: all such communications will be professional in tone and manner
- To protect the privacy of others I will only store confidential child information, personal child information or data on a device that is encrypted or protected with a strong password. I will ensure that school computers are fully logged off or the screen is locked before being left unattended.
- I will report immediately any accidental loss of confidential information so that appropriate action can be taken.
- I will not use my personal mobile phone or other personal electronic equipment to take photographs or videos of children.
- I will only use school equipment to take any photographs or videos of children, with their consent
- I will not use my personal mobile phone or access social media accounts or any website or personal email when with the children.
- I will follow the staff Code of Conduct in regards to school technology
- Any remote work I do away from the school building will be encrypted
- I understand that any personal mobile devices are filtered when used through the school network
- I will treat all equipment belonging to the school with respect and care.
- I understand that the School's digital technology systems are primarily intended for educational use and that I shall only use the systems for personal or recreational use within the rules set out in the School's Staff Code of Conduct

I understand that the school may monitor or check my use of school based ICT equipment and electronic communications.

I understand that by not following these rules I may be subject to the School's disciplinary procedures.

Name ……..

Signed ……

Date ……

Appendix 4

Volunteer or Visitor with access to the Network Acceptable Use Agreement

Richmond House School

ICT and the related technologies such as email, the internet and mobile devices are an expected part of daily working life in school. This agreement is designed to ensure that all visitors are aware of their responsibilities when using any form of ICT. All volunteers and visiting professionals who have access to the school network are required to read and sign this agreement and will specifically adhere to the following points in relation to their own conduct.

- I understand that school ICT equipment, including computers, laptops, digital cameras, mobile phones and any other form of communication technology, is provided by the school for the purposes of teaching and learning, and/or ensuring pupils' safety.
- I understand that I am not permitted to use my personal mobile phone or handheld ICT device during working hours while teaching or supervising pupils, unless in exceptional circumstances.
- I will not install any software or hardware on school ICT equipment without permission.
- I will ensure that all personal data (such as data held on SIMS) is kept secure and is used appropriately. Personal data can only be taken out of school or accessed remotely when authorised by the Head.
- I understand that my use of school information systems, including the internet and email, can be monitored and logged and can be made available, on request, to the Headteacher
- I understand that my own personal digital or mobile cameras are expressly forbidden to be used in school.
- I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner.
- I will respect copyright and intellectual property rights.
- I will comply with the ICT system security and not disclose any passwords provided to my school. I understand that I am responsible for all activity carried out under my user name.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- I will report any incidents of concern regarding children's safety to the online safety Coordinator, the Designated Safeguard Lead or Headteacher.

Signed: _____ Print name: _____

Purpose of visit: _____ Date: _____

APPENDIX 5

Use of Mobile Phones and Cameras for EYFS

Richmond House School EYFS allows staff to bring in personal mobile telephones and devices for their own use.

Staff bringing personal devices into Nursery and Reception must ensure there is no inappropriate or illegal content on the device.

All staff must ensure that their mobile phones/devices are locked away throughout contact time with children.

Mobile phone calls may only be taken out at staff breaks or in staff members' own time. If staff have a personal emergency, they are free to use the school's phone or make a personal call from their mobile either outside or in the Staff Room (where no children are present).

If any member of staff has a family emergency or similar and are required to keep their mobile phone to hand, prior permission must be sought from the Headteacher.

Cameras

Photographs are taken for the purpose of recording a child or group of children participating in activities or celebrating their achievements. It is an effective form of recording their progression in EYFS.
They may also be used on the School website and/or by the local press with permission from the parents. However, it is essential that photographs are taken and stored appropriately to safeguard the children in the School's care.

Only the designated Nursery and Reception cameras and iPads are to be used to take any photos within school or on outings. Images taken on this camera must be deemed suitable without putting the children in any compromising positions that could cause embarrassment or distress.

All staff are responsible for the location of the camera and iPads; these should be put away securely at the end of the day. Images can be shared on ClassDojo pages by EYFS or Specialist teaching staff to share the learning journey with parents and carers.

Under no circumstances must cameras of any kind be taken into the washrooms. If photographs need to be taken in a bathroom, e.g. photographs of the children washing their hands, then the EYFS Phase Leader must be asked first and staff be supervised whilst carrying out this kind of activity.
Failure to adhere to the contents of this policy will lead to disciplinary procedures being followed.

Appendix 6

Internet Safety Concern Form

This form is for use by any adult working in school that has a concern about internet safety. This could be a concern about something witnessed in a lesson or that a child has disclosed to you about something that has happened while using the internet at school or elsewhere.

Date:	Time:
Name of child/adult:	Class:
Setting:	
Other adults present (please complete another form independently)	
Description/Nature of Incident/Concern	
Action Taken (including who this was referred to and when):	
Reported by: Signed	Name and Position
Actioned by: Signed	Name and Position

Appendix 7

InCtrl
Online Sexual Abuse Prevention Service: Key information for professionals

Context

InCtrl is a service for the prevention of sexual abuse. InCtrl (a name chosen by young people) adopts a holistic approach to help build children's digital resilience and support their online and offline relationships and emotional wellbeing.

It helps parents to gain an understanding of the potential risks that exist for children online so they can provide guidance, support and protection when needed. Increasing parental knowledge and confidence to support and protect children. An evaluation for the InCtrl groupwork service was undertaken in 2019-20 with positive findings (McConnell et al., 2020[1]). InCtrl was initially developed as a face-to-face groupwork service but was adapted for individual, virtual delivery during the COVID-19 pandemic.

The service

InCtrl aims to increase safe online behaviours and the digital resilience of children aged 9–13 during the transition period from primary to secondary school - the point where children's use of technology often increases (Ofcom, 2019; 2021[2]). InCtrl practitioners work with children and their parents/carers to build resilience and raise awareness of risks and opportunities in the child's online and offline world.

The programme aims to reduce the likelihood of experiencing technology-assisted child sexual abuse (TA-CSA) or involvement in technology-assisted harmful sexual behaviour (TA-HSB). InCtrl is a child sexual abuse prevention service for children for whom there may be concerns about their online activity or experiences. It can be delivered as a group work or individual, virtual or face-to-face intervention depending on the child's needs.

Group support

The InCtrl consists of weekly face-to-face sessions. The programme is designed to offer a safe space to promote learning, build understanding of risk and increase resilience online and offline.

One to one support

We recognise that for some children a group and/or face-to-face setting may not be suitable. In these cases, 1-2-1 and/or virtual sessions can be offered. One-to-one sessions may be suitable for:

- Children who have social anxiety and/or are shielding.
- Children who have specific learning or emotional needs that mean they may respond better to 1-2-1 support.

The service uses social education to explore children's experiences online and offline. For example, exploring the fluidity and interconnectedness of online and offline spaces and how experiences in one can impact another.

---

[1] McConnell et al. (2020). *Increasing safety and the resilience of children at risk of technology-assisted child sexual abuse.* NSPCC Learning.
[2] Ofcom *Children and parents: Media use and attitudes report* 2019 and 2020/21

NB the content will be treated in a way that is sensitive to the children's age and stage of development.

Session content

The sessions cover the following topics:

1. Session overview
2. Session 1: Introductions and group agreement
3. Session 2: Friendships and relationships online
4. Session 3: How we act online
5. Session 4: Social media, pressure and expectations
6. Session 5: Fear of Missing Out
7. Session 6: Building resilience
8. Session 7: Well-being and self-esteem
9. Session 8: When something feels uncomfortable
10. Session 9: Safety planning

Engaging parents and carers

Research shows that online safety interventions are more effective when parents and carers are involved. Offering an intervention that extends support to parents/carers greatly benefits outcomes for children and contributes to a more holistic offer of support.

There is an expectation that parents and carers will be involved in the InCtrl programme. We will offer support to increase their understanding of the issues facing their children and build on their capacity to offer support and protection to their children. This may include exploring children's previous experience of adversity and how this may have an impact on their experience of relationships and further risks.

Practitioners will undertake a home visit or a virtual meeting to introduce themselves and explain the service. There is also an option of a parents' group meeting where appropriate.

The content for parents and carers reflects the child's sessions to ensure children are given a consistent message, and to help parents and carers in support their child to be safe online.

How to make referrals to this service

Pre-referral meeting

Prior to making a referral you should arrange to speak with one of our InCtrl practitioners and discuss the service in more detail to find out more about the child's needs, eligibility for the service and support you to identify (and complete where required) potential referrals. The InCtrl practitioner will provide you with information to share with the child and their parent/carer.

If InCtrl is suitable for the child you will then complete *NSPCC standard request for service* form with one our InCtrl practitioners and other things such as a Working Together Agreement.

We ask that the child and their parents/carers are informed and included in the referral process. Referrals can only be made with consent from both.

Referral process and consent

Our InCtrl assessment and referral form asks for detail about the child to help us ensure they are offered the intervention best suited to their needs. It also begins the assessment process completed in the first session and allows us to consider how best to adapt the intervention to the child's needs.

Where possible, we ask that you involve the child and their parents/carers in the completion of the *NSPCC standard request for service* form (i.e. the referral form). It is expected that you will discuss the referral form with them as a minimum, and be prepared to share the referral form with the child and their parents/carers so they are fully aware of what you have shared. We recognise that this is their private and personal information, and we will manage it sensitively to support trauma informed approaches from the beginning. We can help you to navigate this if it presents any challenges.

An individual assessment and referral form must be completed for each child, including those being referred as a group. If you are referring a group of young people we ask that these referrals come from one source. Given the sensitive nature of some content it is helpful for children to have an additional source of support, alongside the NSPCC, during the intervention. However, an individual referral form should be completed for each child within the group.

If you have any questions about this service or are interested in referring a child please get in touch with one of our InCtrl practitioners.