E-Safety Policy

Introduction

Technology plays an important role at Hopespring Education. It is often used within lessons as a central resource to help with the educational development of our students. Furthermore, it helps with the administrative side of our work with young people.

However, whilst the educational possibilities of using ICT are rapidly developing, all users of technology need to be aware of the potential dangers and risks associated with its use.

At the school, we understand the responsibility to educate our students on eSafety issues; teaching them appropriate behaviour and skills to enable them to remain both safe and legal whilst using technology.

This policy aims to highlight some of the issues associated with ICT and provides guidance on how ICT should/could be used.

Roles and Responsibilities

As eSafety is an important aspect of strategic leadership within the school, the Centre Manager and Management Committee have ultimate responsibility to ensure that the policy and practices are embedded and monitored. All members of the school community need to be aware of the key people responsible for eSafety. At least one member of the Management Committee needs to have undertaken training by a recognised organisation to deal with issues relating to eSafety and to allow training to be given to staff.

There is an expectation that the Centre Manager/Deputies and Management Committee regularly access this policy on an annual basis. It is their duty to ensure they have an understanding of the issues and strategies at their school in relation to local and national guidelines and advice.

This policy, supported by the school's acceptable use agreements for staff, Management Committee members, visitors and students, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies on safeguarding and child protection, health and safety, student conduct agreement, and behaviour (including the anti-bullying) policy and PSHE.

Monitoring

Authorised ICT support staff may access ICT equipment that is owned/leased by the school at any time with prior notice. Generally, this will be completed by a representative from the ICT support service provider for the school.

In certain circumstances the Centre Manager or a senior member of staff may instruct the service provider to monitor, intercept, access, inspect, record and disclose emails, instant messaging, internet/intranet use and any other form of electronic communication involving any student or employee, without consent, to the extent permitted by law.

Occasions where this may be necessary include:
- Confirming or obtaining school business related information
- Confirm or investigate compliance of school standards, policy and procedures
- Quality control or training purposes
- Prevent or detect crime
- Child protection

All monitoring, investigative and surveillance work should be conducted by authorised ICT staff and comply with the Data Protection Act 1998, Human Rights Act 1998, Regulation of investigatory Powers Act 2000 and the Lawful Business Practice Regulations 2000.

All Internet activity is filtered by our internet firewall provider (KBR). Browsing history may be monitored by the school if there are suspicions of misuse. The School uses Senso Cloud software to filter internet use and to view and control student computer use.

Acceptable use agreements

Each year, ALL staff employed at the school shall undertake some training with regards to eSafety. As part of this training, all employees should sign an Acceptable Use Agreement and this must be held by the Centre Manager.

All students should take part in one dedicated lesson at the start of the year where eSafety is addressed and students re-sign an acceptable use agreement. A copy of the staff, pupil and parent agreements can be found in the appendices of this policy.

Parents should be alerted to the eSafety policy during the referral interview, through the *referral form* and should be made available as a hard copy or electronically if requested. The eSafety policy and additional information related to eSafety is accessible from the school website. Parents should sign up to the school policy during the referral interview before their child starts.

Security

This Policy is intended to minimise security risks. These risks might affect the integrity of the school's data, the authorised user and the individuals to which the data pertains. In particular, these risks arise from:

- The intentional or unintentional disclosure of login credentials to by authorised users
- The wrongful disclosure of private, sensitive and confidential information
- Exposure of Hopespring to vicarious liability for information wrongfully disclosed by authorised users.

Data Access

This Policy aims to ensure all relevant aspects of the GDPR 2018 are adhered to. This Policy aims to promote best use of our systems to further the communication and freedom of information between the school and Parents/Carers.

Data Usage Policy Rules

Authorised Users

Our IT systems are provided for use only by persons who are currently employed by the school, and for students. Access to the functions of the system and information contained within it is tailored dependent on the roles and responsibilities of the user.

Personal Use

Information made available through our database is confidential and protected by law under the Data Protection Act 1998. To that aim:

- Users must not distribute or disclose any information obtained from our systems to any person(s) with the exception of the students to which the information relates or to other adults with parental responsibility.
- Users should not attempt to access our databases in any environment where the security of the information contained in them may be placed at risk, e.g. a cybercafé.

Password Policy

You must assume personal responsibility for your username and password. Never use anyone else's username or password. You must always keep your individual username and password confidential. These usernames and passwords should ***never*** be disclosed to anyone. Passwords and usernames should never be shared.

Passwords for any users other than students, will be issued by HR and cannot be changed by the user. Passwords for students will be issued by school staff and can be changed by staff.

Hopespring reserves the right to revoke or deny access to the IT systems of any individual under the following circumstances:
- Users found to be in breach of this policy
- Users no longer employed by the school.

If any child protection concerns are raised or disputes occur, the school may revoke

access for all parties concerned pending investigation.

Users are liable for any potential misuse of the system and/or breach of the data protection act that may occur as a result of failing to adhere to any of the rules/guidelines listed in this document.

Email System – Staff

The use of email within the school is an essential means of communication for staff. In the context of the school, e-mails CANNOT be considered as private and should therefore only be used for official school business.

- The school gives each member of staff an email account in order to protect staff and minimise the risk of receiving malicious / unsolicited emails.
- All email may be filtered and logged and email histories may be re-traced. Therefore it should only be used for official school business
- Users should keep passwords and account details secure.
- Students/parents/carers should, under no circumstances, be contacted by staff using their personal email address.
- When sending an email from a school account, it should include the standard disclaimer statement. This is to protect the school and ensure personal responsibility from the user.
- Emails should be carefully checked before sending as any content signifies official school correspondence, similar to that of letters being sent using letter headed paper.
- Emails created on a school account will be subject to disclosure should a request be made under the Freedom of Information Act 2000.
- Staff MUST inform their line manager/eSafety coordinator of any offensive emails they receive.
- Send emails to intended recipients only. Do not send blanket emails unnecessarily.
- Only send attachments to intended recipients.
- Check emails regularly and delete unwanted items.
- Never open attachments from unwanted / unknown sources.

Email for School Students

The school does not provide a dedicated in-house email system for students. Students who are aged 13 and over, may register for a gmail account for use in ICT lessons. Students may not do this until they have covered safe use of the system in a dedicated ICT lesson. Students may also use email accounts provided by their referring schools.

- Student users are expected to adhere to general good practice guidelines of netiquette (delivered in ICT lessons). Language should be appropriate and they should not reveal any personal information about themselves to other people.
- At KS3, students should use emails under general supervision and should form a structured part of the lesson.
- At KS4, students may use email more freely but staff should still regulate its use in lessons.

eSafety in the ICT and PSHE Curriculum

eSafety is securely embedded into the ICT curriculum. It is essential for students to receive the same message across faculty areas and to learn the skills necessary for staying safe using ICT. Below are some areas covered in the ICT Curriculum.

- Staying Safe online, including recognising and guarding against radicalisation
- Social Networks
- Cyberbullying
- Copyright and keeping information safe and secure
- Legislation relating to computers and technology
- Respecting information
- Using correct and appropriate search techniques
- Sexting

Cross Curricular eSafety

ICT now plays a key part in the education of students. ICT is used widely for research and to enhance the quality of work produced by students. It is important that teaching and learning incorporates the use of ICT and that when planning and delivering lessons using ICT, matters relating to eSafety are considered by all staff.

Staff Training

Training will be provided annually to all staff as part of the introduction to the new school

year. This will be focussed on keeping students safe and managing risk. Regular information on eSafety will be provided to staff to keep them abreast of developments.

Over the school year, there may be opportunities for staff to attend additional training events. Information about these will be published when available.

All staff will review the acceptable use agreement on an annual basis and sign the document to acknowledge their professional responsibilities in relation to ICT in general. New staff starting midyear will need to sign this as part of their induction.

Use of the Internet

Staff and students are able to access a wealth of information via the Internet to help with education/study. It is important though that the Internet is not used excessively and is well planned into the curriculum. The School provides students with supervised access to internet resources through the use of Senso Cloud software. Websites and their content are filtered by Senso Cloud and staff can add to the list of blocked sites flexibly and quickly.

Staff should preview any recommended sites before use to check that they work on the school system and are appropriate, including checking that they do not contain any terrorist or extremist material.

Raw image searches are discouraged when working with students and key search terms are provided to students.

If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research.

All users must observe software copyright at all times. It is illegal to copy or distribute school-owned software or illegal software from other sources.

All users must observe copyright of materials from electronic resources.
The Internet should be used primarily for educational purposes. Where students are given permission to use the Internet recreationally, close supervision must be given to the sites

they are visiting and content they are viewing. Should you come across a website that is inappropriate it is important to block it locally using Senso Cloud.

There should be no attempt to access sites deemed inappropriate as this will trigger an alert on the monitoring system. If any pupil uses the Internet inappropriately, this should be logged with the Centre Manager and the eSafety Lead should be made aware of all significant or ongoing concerns.

There are a number of resources (see Appendix B) to support staff, parents and carers in discussing internet safety with users.

Use of Digital Images and Video

Digital images are easy to capture, reproduce and publish and, therefore, misuse. It is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.

- Not all parents' give permission for photographs of students to be taken. This information can be found on the referral documents and must be adhered to as there are often safeguarding reasons why photographs should not be taken and used.
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of students, this includes when on field trips. If the school has a mobile phone for staff use that belongs to the centre and remains in the centre then this may be used to photograph students. Students are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of students, staff and others without advance permission from the Centre Manager.
- Where digital images/photographs are used and shared publicly, students' first names only should be used.

Social Networks

Facebook, Twitter, Snapchat, Instagram, YouTube, Whatsapp, online gaming and other

forms of social media are increasingly becoming an important part of our daily lives. However, our students often misuse social networks which cause issues at the school. In addition, there is an increased risk of online radicalisation, as terrorist organisations such as ISIL seek to radicalise young people through the use of social media and the internet. Therefore, the use of social networks at the school is not allowed and students take part in lessons highlighting the risks when using the internet and social networks in their own time.

- Staff are not permitted to access their personal social media accounts using school equipment during working hours. If staff are using school equipment to access social media outside of work hours, they must be mindful of the fact that data will be stored locally within the device history, that they need to log out at the end of the session and that login details should not be auto-filled or remembered by the device.
- Students are not permitted to access their social media accounts whilst at school on ANY device be it school equipment or that of their own.
- Staff, management committee, students, parents and carers are regularly provided with information on how to use social media responsibly and what to do if they are aware of inappropriate use by others
- Staff, management committee, students, parents and carers are aware that the information, comments, images and video they post online can be viewed by others, copied and stay online forever.
- Staff, management committee, students, parents and carers are aware that their online behaviour should at all times be compatible with UK law.
- Staff should not befriend current students on social networking sites and best practise is to wait until that pupil is 19 before doing so (if necessary).

Mobile Telephones

Mobile phones can be used for music in the classroom. Phones may be confiscated if they are felt to be being used in a disruptive way. Disruptive ways include causing students to not listen, stopping you doing a task or disrupting other people. they may also be confiscated if a student is using them to access and share inappropriate material. There should be no need for students to make or receive calls from their mobiles in the school – all phone calls should be made or received on the School Phone.

Misuse of ICT

- Complaints of Internet Misuse must be reported and dealt with by the Centre

Manager or Management Committee.

- Any complaint about staff misuse should be directed to the Centre Manager or the Management Committee.
- Complaints of a child protection nature should be referred in the usual manner to the school-based Designated Safeguarding Lead.

Relevant Legislation

Acts Relating to Monitoring of Staff email

- **General Data Protection Regulations 2018**

  The Regulations require anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. It grants individuals rights of access to their personal data, compensation and prevention of processing.

  http://www.hmso.gov.uk/acts/acts1998/19980029.htm

- **The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000**

  http://www.hmso.gov.uk/si/si2000/20002699.htm

- **Regulation of Investigatory Powers Act 2000**

  Regulating the interception of communications and making it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.

  http://www.hmso.gov.uk/acts/acts2000/20000023.htm

- **Human Rights Act 1998**

  http://www.hmso.gov.uk/acts/acts1998/19980042.htm

Other Acts Relating to eSafety

- **Racial and Religious Hatred Act 2006**

  It a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

- **Sexual Offences Act 2003**

  The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. Schools should already have a copy of "*Children & Families: Safer from Sexual Crime*" document as part of their child protection packs.
  For more information www.teachernet.gov.uk

- **Communications Act 2003 (section 127)**

  Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

- **The Computer Misuse Act 1990 (sections 1 – 3)**

  Regardless of an individual's motivation, the Act makes it a criminal offence to gain access to computer files or software without permission (for example using another person's password to access files,)unauthorized access, as above, in order to commit a further criminal act (such as fraud) impair the operation of a computer or

program. UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

- **Malicious Communications Act 1988 (section 1)**
  This legislation makes it a criminal offence to send an electronic message (e-mail) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

- **Copyright, Design and Patents Act 1988**
  Copyright is the right to prevent others from copying or using work without permission. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer. Copyright infringement is to copy all or a substantial part of anyone's work without obtaining them author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

- **Public Order Act 1986 (sections 17 – 29)**
  This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

- **Protection of Children Act 1978 (Section 1)**
  It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

- **Obscene Publications Act 1959 and 1964**
  Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

- **Protection from Harassment Act 1997**
  A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Acts Relating to the Protection of Personal Data

- **General Data Protection Regulations 2018**

  https://gdpr-info.eu/

- **The Freedom of Information Act 2000**

  http://www.ico.gov.uk/for_organisations/freedom_of_information_guide.aspx

Appendix A: Codes and Agreements

(page left blank)

E Safety – Staff Code of Conduct for ICT

To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with students, they are asked to sign this code of conduct. Members of staff should consult the school's e-safety policy for further information and clarification.

- ❏ I understand that it is a criminal offence to use the school's system for a purpose not permitted by its owner.
- ❏ I appreciate that ICT includes a wide range of systems, including mobile phones, tablets, PDAs, digital cameras, email, social networking and that ICT use may also include personal ICT devices when used for school business.
- ❏ I understand that the school's information systems may not be used for private purposes without specific permission from the Centre Manager.
- ❏ I understand that my use of the school's information systems, internet and email may be monitored and recorded to ensure policy compliance.
- ❏ I will respect security and I will not disclose any password or security information to anyone other than an authorised system manager.
- ❏ I will not install any software or hardware without permission.
- ❏ I will ensure that personal data is stored securely and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- ❏ I will respect copyright and intellectual property rights.
- ❏ I will report any incidents of concern regarding children's safety to the e-Safety Lead, and the Designated Safeguarding Lead.
- ❏ I will ensure that electronic communications with students including email are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
- ❏ I will ensure that my personal use of the school's systems (e.g social networking, text messaging) will not crossover with my ICT use professionally by protecting my social networking profiles from public view and not giving out personal contact information. **I will not add current students as friends on social networking sites, and will take care to ensure that any comments about the school/school activities are appropriate and professional.**

(PTO)

The school may exercise its rights to monitor the use of the school's information systems and internet access, to intercept email and to delete inappropriate materials where it believes unauthorised use of the school's information systems may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood and accept the Staff Code of Conduct for ICT.
Signed: _____
Print name: _____
Date: _____

E Safety – KS3/4 Pupil Acceptable Use Agreement

These rules will keep everyone safe and help us to be fair to others.

❑ I will only use the school's IT equipment for appropriate school activities and learning and am aware that the school can monitor my internet-use.

❑ I will not bring files into school that can harm the school network or be used to circumvent school security tools.

❑ I will only edit or delete my own files and not view, or change, other people's files or user areas without their permission.

❑ I will keep my logins, IDs and passwords secret and change my password regularly.

❑ I will use the Internet responsibly and will not visit websites that are inappropriate for the school or my key stage.

❑ I will only email or contact people I know, or those approved as part of learning activities.

❑ The messages I send, or information I upload, will always be polite and sensible. All messages I send reflect on me and the school.

❑ I will be careful when opening files and attachments, checking for viruses etc. If I am unsure I will never open a file.

❑ I will not give my personal information that could be used to identify me, my family or my friends on any online space, unless a trusted adult has given permission or reviewed the site.

❑ I will never arrange to meet someone I have only ever previously met on the Internet or by email or in a chat room, unless I take a trusted adult with me.

❑ If I see anything I am unhappy with or I receive a message that makes me feel uncomfortable, I will not respond to it but I will save it and talk to a trusted adult.

❑ I am aware that some websites, games and social networks have age restrictions and I should respect this.

❑ I am aware that my online activity at all times should not upset or hurt other people. This includes not taking and sharing of images of staff or other students which could be used to offend or deliberately hurt or upset them. I'm aware that procedures are in place to protect staff and students from this activity and that action will be taken against anyone who disregards this agreement.

I have read, understood and accept the Acceptable Use Agreement for ICT.
Signed: _____
Print name: _____
Date: _____

E Safety – Parent/Carer Agreement Form

Internet and ICT: As the parent or legal guardian of the pupil(s) named below, I grant permission for the school to give my child access to:

- the Internet at school,
- the school's chosen email system,
- ICT facilities and equipment at the school.

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school takes every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials.

I understand that the school can, if necessary, check my child's computer files and the Internet sites they visit at school and if there are concerns about my child's e-safety or e-behaviour they will contact me.

Use of digital images, photography and video:
I understand the school has a clear policy on "The use of photographs" within the E-Safety Policy and I support this.

If I have given permission, I understand that the school may use photographs of my child or include them in video material to support learning activities.

If I have given permission, I accept that the school may use photographs/video that includes my child in publicity that reasonably promotes the work of the school, and for no other purpose.

I will not take and then share online, photographs of other children (or staff) at school events without permission.

(PTO)

Social networking and media sites:
I understand that the school has a clear policy on "The use of social networking and media sites" and I support this.

I understand that the school takes any inappropriate behaviour seriously and will respond to observed or reported inappropriate or unsafe behaviour.

I will support the school by promoting safe use of the Internet and digital technology at home. I will inform the school if I have any concerns.

I have read, understood and accept the E Safety – Parent/Carer Agreement Form.

My child's name: _____

Signed: _____

Print name: _____

Date: _____

Appendix B - Online Safety Resource for Staff, Parents and Carers

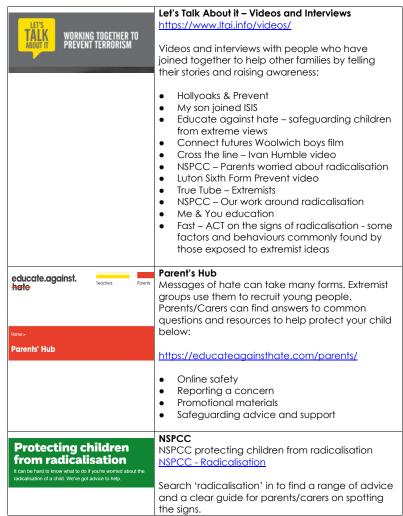|	
UK Safer Internet Centre logo	**UK Safer Internet Centre** https://www.saferinternet.org.uk/ https://www.saferinternet.org.uk/advice-centre/parents-and-carers ● Online safety tips, advice and resources to help children and young people stay safe online. ● Lesson plans, films, games, quizzes, drama activities and more
internet matters.org In partnership with BT	**Internet Matters: Helping parents keep children safe on line.** https://www.internetmatters.org/ ● School resources (Early Years, Primary & Secondary) ● Advice by age ● Setting online controls ● Guides & resources - Updated for COVID-19 ● https://www.internetmatters.org/resources/staysafestayhome-tech-advice-for-families/ ● Specific content around radicalisation ● https://www.internetmatters.org/?s=radicalisation
LET'S TALK ABOUT IT — WHAT IS PREVENT? SPOTTING THE SIGNS CONTACT	**Let's Talk About it (LTAI)** https://www.ltai.info/ LTAI is an initiative designed to provide practical help and guidance in order to stop people becoming targeted by terrorists or supporting terrorism. Highlighting issues and initiating discussions around the potential threats we face as a community today. Together we can create greater understanding and wider awareness to help protect our young people.

LET'S TALK ABOUT IT — WORKING TOGETHER TO PREVENT TERRORISM	**Let's Talk About it – Videos and Interviews** https://www.ltai.info/videos/ Videos and interviews with people who have joined together to help other families by telling their stories and raising awareness: ● Hollyoaks & Prevent ● My son joined ISIS ● Educate against hate – safeguarding children from extreme views ● Connect futures Woolwich boys film ● Cross the line – Ivan Humble video ● NSPCC – Parents worried about radicalisation ● Luton Sixth Form Prevent video ● True Tube – Extremists ● NSPCC – Our work around radicalisation ● Me & You education ● Fast – ACT on the signs of radicalisation - some factors and behaviours commonly found by those exposed to extremist ideas
educate.against.hate Teachers / Parents — Home > Parents' Hub	**Parent's Hub** Messages of hate can take many forms. Extremist groups use them to recruit young people. Parents/Carers can find answers to common questions and resources to help protect your child below: https://educateagainsthate.com/parents/ ● Online safety ● Reporting a concern ● Promotional materials ● Safeguarding advice and support
Protecting children from radicalisation It can be hard to know what to do if you're worried about the radicalisation of a child. We've got advice to help.	**NSPCC** NSPCC protecting children from radicalisation NSPCC - Radicalisation Search 'radicalisation' in to find a range of advice and a clear guide for parents/carers on spotting the signs.

Addendum 1: Hopespring Sunderland 10 Sea View particulars (if applicable)

Addendum 2 Hopespring Sunderland Millfield particulars (if applicable)

Addendum 3: Hopespring Newcastle particulars (if applicable)