LANCASTER
STEINER SCHOOL

Online Safety Policy

Version date: July 2020

Document review date: From September 2021

LSSOLP/004/2018

POLICY STATEMENT

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education (Sept 2019) and its advice for schools on preventing and tackling bullying. It also refers to the Department's guidance on protecting children from radicalisation. It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010.

The use of technology has become a significant component of many safeguarding issues. Child sexual exploitation; radicalisation; sexual predation: technology often provides the platform that facilitates harm. An effective approach to online safety empowers a school or college to protect and educate the whole school or college community in their use of technology and establishes mechanisms to identify, intervene in, and escalate any incident where appropriate. The breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk:

• **Content:** being exposed to illegal, inappropriate or harmful material; for example, pornography, fake news, racist or radical and extremist views.

• C**ontact:** being subjected to harmful online interaction with other users; for example, commercial advertising as well as adults posing as children or young adults; and

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

This Online Safety Policy has been agreed by the College of Teachers, Trustees and Safeguarding leads.

Safeguarding is taken very seriously and this document outlines and clarifies to the way in which Online Safety is to be addressed by both pupils and staff at Lancaster Steiner School (LSS).

The primary purpose of this policy is twofold:

- *To ensure the requirement to empower the whole school community with the knowledge to stay safe and risk free is met*
- *To ensure risks are identified, assessed and mitigated (where possible) in order to reduce any foreseeable harm to students, staff, parents, users and the wider school community or liability to the school.*

This policy is available for anybody to read and is available on the LSS website, upon review all members of staff will sign as read and understood both, the Online Safety Policy, Whole School Behaviour Policy and the Acceptable Use Policy (AUP).

Online safeguarding, known as Online Safety, is an area that is constantly evolving and as such this policy will be reviewed on an annual basis or in response to an online safety incident, whichever is sooner.

GLOSSARY

For clarity, the Online Safety policy uses the following terms, unless otherwise stated.

Lancaster Steiner School: LSS

SGT: Senior Governance Team includes the Trustees, Education and Teacher Coordinators, Early Years Lead and the School Manager

Management Team: Education and Teacher Coordinators, Early Years Lead and the School Manager

Users: Refers to staff, governing body, school volunteers, students and any other person working in or on behalf of the school, including contractors.

Parents: Any adult with a legal responsibility for the child/young person outside the school e.g. parent, guardian, carer.

Pupils: Kindergarten, Lower School Class T to 5,

School: Any school business or activity conducted on or off the school site, e.g. visits, meetings, school trips etc.

Wider school community: Parents, visitors & relatives

Trustee with responsibility for Safeguarding: Sara Nobili Park

Designated Safeguarding Leads: (DSL) Ola Mustapha; Deputy DSL's Rachel Theobald & Elspeth Mukerji

Local Authority Designated Officer: Tim Booth, Shane Penn and Donna Green of LADO Lancashire County Council, 01772 536694, LADO.admin@lancashire.gov.uk

ROLES AND RESPONSIBLITIES

SCHOOL GOVERNANCE TEAM (SGT)

The SGT has overall responsibility for monitoring this policy and holding the management team to account for its implementation. Online Safety and the monitoring of any online safety concerns, will be discussed as part of regular Safeguarding meetings which are attended by the Trustee with responsibility for Safeguarding, Designated Safeguarding Lead and the Deputy Safeguarding Lead. All trustees will:

• Ensure that they have read and understand this policy

• Agree and adhere to the terms of Acceptable Use of the school's ICT systems and the internet

The Management Team is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

Details of the school's designated safeguarding lead (DSL) are set out in our safeguarding policy.

The DSL takes lead responsibility for online safety in school, in particular:

• Supporting the management team in ensuring that staff understand this policy and that it is being implemented consistently throughout the school

• Working with the staff, as necessary, to address any online safety issues or incidents

• Ensuring that any online safety incidents are logged and dealt with appropriately in line with the Acceptable Use Policy (ICT).

• Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the Whole School Behaviour Policy

• Ensuring that staff undertake and regularly update training on online safety

• Liaising with other agencies and/or external services if necessary

• Provide regular reports as part of the SG meetings

The school provides the following measures to ensure reasonable steps are in place to reduce the risk of harm to pupils, staff and the school through:

- Ensuring that personal information is not published
- Regular staff training in Child Protection, PREVENT, Online Safety and Peer on Peer Abuse Awareness Training accessed on Educare, as outlined in the rolling training programme (any additional training, such as Child Sexual Exploitation, will be accessed on Educare as deemed necessary by the DSL)
- Clear reporting guidance including responsibilities, procedures and sanctions
- Issuing all staff with an LSS Staff Handbook, and our Code of Conduct and the Employee Handbook which includes Social Media Policy, the use of Computer and Electronic devices in addition to the school's Acceptable Use Policy (ICT)
- Ensuring all staff read and sign our Bring Your Own Devices and Acceptable Use Agreements which are included in the Acceptable Use Policy (ICT)

STAFF

All staff are expected to

- read and sign the Acceptable Use Policy and Online Safety Policy before using any school ICT resources
- lead by example, and have an up to date awareness of Online Safety matters, current school policies and practices
- familiarise with current issues and guidance through organisations such as, CEOP (Child Exploitation and Online Protection) and ChildNet (forwarded by DSL)
- report misuse or problems to DSL for investigation
- understand that digital communications with pupils on roll are not permitted
- deliver our online safety curriculum
- keep electronic devices in the staff room or office at all times except in exceptional circumstances as outlined in the Acceptable Use Policy (ICT)

- ensure that all digital communications with staff and parents should be on a professional level
- register their electronic devices on an Acceptable Use agreement. Members of staff can then use their device to capture children's work, but only class teachers and the admissions officer can use their devices for capturing images of children and only when they have registered their device with a Bring Your Own Devices agreement and their device is not linked to to any virtual storage such as icloud or googlemail. The office must be notified prior to taking the device into an area where the children are situated, all pictures will be TRANSFERRED by the staff member onto the school hard drive, and then all photos must be deleted before leaving the school premises with their device. (For more information see the Use of Image Policy)
- abide by the Social Media Policy (Employee Handbook) and Acceptable Use Policy (ICT)
- keep parents regularly updated about online safety

SCHOOL MANAGER

The School Manager will coordinate office staff to

- maintain a current record of anyone who are granted access to the school' s electronic communications
- carry out inductions with all new volunteers, staff and trustees
- ensure that the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- ensure that users may only access the school's computers through a properly enforced password protection policy, in which passwords are regularly changed
- keep up to date with technical information, in order to effectively carry out their role
- keep abreast of current issues and guidance through organisations such as, CEOP (Child Exploitation and Online Protection) and ChildNet.

PUPILS

Phones are only to be brought into school only when absolutely necessary, with prior agreement parents are to inform the school in writing stating the reason. In this instance pupils are to hand their phone in to the office at the beginning of the school day, and it will be kept in the office till needed.

Pupils are not allowed to bring a mobile phone into school, unless in exceptional circumstances and with agreement with the school (see section Cameras, Mobile Phones and Devices in the Safeguarding Policy). However, were the need to search a pupil for a mobile device arise, DfE advice: Searching, Screening and Confiscation will be followed. A copy of this departmental advice is kept in the School's Safeguarding Portfolio.

If pupils are using devices with their class teacher as part of the curriculum then they are expected to only access the resources /materials they have been asked to use under direct supervision

PARENTS, CARERS AND VISITORS

Parents are expected to;

- inform school immediately of any concerns regarding Online Safety
- support the ethos of the school – which stresses the importance of the human relationship and the spoken word in the primary years – and to protect individual privacy, we strongly ask parents/carers not to use mobile phones in school when dropping off or collecting children
- make sure their own use of ICT, for example mobile phones, laptops, and cameras when in school or with school on trips, festivals, walks and visits is appropriate as outlined in the school Acceptable Use agreement
- refrain from using mobile phones inside school premises (except for the school yard)
- ensure that no pictures of pupils other than their own children are posted on social networking sites without direct permission from the parent of the pupils concerned
- follow the complaints procedure rather than posting complaints on social networking sites
- not post malicious or fictitious comments on social networking sites about any member of the school community.
- any comments on social media sites that could be interpreted as bringing the school into disrepute will be handed to the Local Authority Legal Team who will decide on an appropriate course of action.
- Read and understand the Acceptable Use Policy (ICT) and sign the Acceptable Use (of Internet) Agreement for parents and carers
- leave all electronic devices with the school office or staff room if staying in school.

Parents are informed of their responsibilities regarding this Online Safety policy during the Educational Interview for their child. This information is also in the Parent Handbook.

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

UK Safer Internet Centre: https://www.saferinternet.org.uk/advicecentre/parentsand-carers/what-are-issues

Hot Topics, Childnet International: http://www.childnet.com/parents-and-carers/hottopics

Parent factsheet, Childnet International: http://www.childnet.com/ufiles/parentsfactsheet-09-17.pdf

The government also provides an online reporting tool for concerns about online ,material that promotes extremism or terrorism which both staff and parents can use http://www.gov.uk/report-terrorism

COMMUNITY USERS

Community Users of the school are not given access to any of the school's IT equipment. They are informed of the school photograph policy.

CURRICULUM

We have an Online Safety Curriculum Framework (see Appendix 2) which will form part of our PSHE curriculum that begins in Kindergarten and covers all aspects of internet use introduced at an age appropriate level.

Pupils are made aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/carer, teacher/trusted staff member, or an organisation such as Childline.

DEALING WITH INCIDENTS

CYBER BULLYING

Cyber bullying can be defined as the use of information and communications technology particularly mobile phones and the internet, deliberately to upset someone else. Cyber bullying that occurs while pupils are under the school's direct supervision will be dealt with in line with this policy, the Safeguarding Policy and the Whole School Behaviour Policy.

In cases where cyber bullying occurs while pupils are outside our direct supervision (i.e. at home), parents will be encouraged to report these incidents to the Police as criminal laws (such as those pertaining to harassment, threatening and menacing communications) may apply. Parents are also encouraged to report such bullying to the school. If the alleged perpetrator is a member of this school community, the school will act in line with the Whole School Behaviour Policy and procedures. The school will, wherever possible, support parents in this and may impose a sanction upon the bully where this individual is recognisable.

The school can take action against incidents that happen outside school, when;

- actions could have repercussions for the orderly running of the school,
- actions pose a threat to another pupil, college of staff, trustee, parent or member of the public which could adversely affect the reputation of the school.

Acts of cyber bullying can include:

- name-calling;
- mocking;
- making offensive comments;
- inappropriate text messaging, emailing or 'posting' on social media sites;
- sexting;
- sending offensive or degrading images by phone or via the internet e.g. via Social media sites;
- excluding people from groups;
- spreading hurtful and untruthful rumours.

ACCEPTABLE USE OF THE INTERNET IN SCHOOL

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role. We reserve the right to monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above. More information is set out in the Acceptable Use Policy (ICT).

The school takes all reasonable precautions to ensure that users access only appropriate material online including the use of filters. However, it is not possible to guarantee that unsuitable material will never appear on a school computer.

The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990

RESPONSE TO A BREACH OF POLICY

A breach or suspected breach of policy by a School employee, contractor or pupil may result in the temporary or permanent withdrawal of School ICT hardware, software or services from the offending individual. Any policy breach is grounds for disciplinary action in accordance with the School Disciplinary Procedure. Policy breaches may also lead to criminal or civil proceedings.

LINKS TO OTHER POLICIES AND DOCUMENTS

This policy forms part of Lancaster Steiner School's policy for safeguarding children. It should also be read alongside:-

- Safeguarding Policy
- Whole School Behaviour Policy
- Data Protection Policy and GDPR 2018
- Keeping Children Safe in Education 2019
- Acceptable Use Policy (ICT) and Bring Your Own Device Agreements
- Use of Image Policy (ICT)

APPENDIX 1

Online Safety Declaration

I_____(full name) confirm I have read and understand the Lancaster Steiner School Online Safety Policy. If I have any questions I should speak to the Safeguarding Lead, Ola Mustapha.

Signed:

Date:

APPENDIX 2

Online Safety Curriculum Framework

Aims of the Framework

1. Self-image and Identity
2. Online relationships
3. Online reputation
4. Online bullying
5. Managing online information
6. Health, wellbeing and lifestyle
7. Privacy and security
8. Copyright and ownership

The framework aims to support and broaden the provision of online safety education, so that it is empowering, building resilience and effects positive culture change. The objectives promote the development of safe and appropriate long term behaviours, and supported educators in shaping the culture within their setting and beyond.

1. Self-Image and Identity	This strand explores the differences between online and offline identity beginning with self-awareness, shaping online identities and how media impacts on gender and stereotypes. It identifies effective routes for reporting and support and explores the impact of online technologies on self-image and behaviour.

Class	Learning Aim	Possible Resources
KG	I can recognise that I can say 'no'/'please stop'/'I'll tell'/'I'll ask' to somebody who asks me to do something that makes me feel sad, embarrassed or upset.	
KG	I can explain why I should keep asking until I get the help I need.	
KG & 1	I can explain how this could be either in real life or online.	
1	I can describe issues online that might make me or others feel sad, worried, uncomfortable or frightened. I know and can give examples of how I might get help, both on and offline.	
1	If something happens that makes me feel sad, worried, uncomfortable or frightened I can give examples of when and how to speak to an adult I can trust.	
2	I can recognise that there may be people online who could make me feel sad, embarrassed or upset.	
2	I can explain what is meant by the term 'identity'.	
2	I can explain ways in which and why I might change my identity depending on what I am doing online (e.g. gaming; using an avatar; social media).	
2	I can explain how my online identity can be different to the identity I present in 'real life'.	

3 & 4	Knowing this, I can describe the right decisions about how I interact with others and how others perceive me.	
4	I make positive contributions to other's self-identity, where appropriate (e.g. avoiding negative comments or positive commentary on profile pictures).	
4 & 5	I can explain how other people's identity online can be different to their identity in real life.	
4 & 5	I can give examples of issues online that might make me feel sad, worried, uncomfortable, or frightened; I can give examples of how I might get help.	
5	I can describe ways in which people might make themselves look different online.	
5	I can identify outline role models who manage a positive identity and give examples from my own research/experience to support my understanding.	

2. Online Relationships	This strand explores how technology shapes communication style and identifies strategies for positive relationships in online communities. It offers opportunities to discuss relationships and behaviours that may lead to harm and how positive online interaction can empower and amplify voice.

Class	Learning Aim	Possible Resources
KG	I can give examples of how people (might) use technology to communicate with people they know.	story
KG	I like meeting new people but know I have to be careful when meeting people I don't know.	story
KG & 1	I can explain why it is important to be considerate and kind to people; when we play, when we work in school, when people talk to each other on the phone or through the computer.	story
KG & 1	I can explain how my and other people's feeling can be hurt by what is said or written.	
KG & 1	I can use the internet with adult support to communicate with people I know; Skype.	Scenario; Granny in Germany
1 & 2	I can give examples of different forms of written communication, cunei form, hieroglyphs. I know that on computers and phones people also use symbols, for example emojis.	
1 & 2	I like meeting new people, but know I have to be careful when meeting people I don't know. When people meet others they don't know well online they are careful too.	
1 & 2 & 3	I can recognise different ways of communicating; talking, smiling, writing, phoning, skyping.	Story; Anna and the dragon
2	I can use the internet to communicate with people I don't know well; (email, pen pal in another school or country).	
2	I can explain why people should be careful who they trust online and what information they can trust them with.	
3	I can give examples of how I might use technology to communicate with others I don't know well.	
3 & 4 & 5	I can explain how my and other people's feelings can be hurt by what is said or written. I can explain how this can particularly happen online.	
4	I can describe ways people who have similar likes and interests can get together for example in the playground, in sport groups. I know that people with a similar interest can also get together online for example through computer games.	Scenarios
4 & 5	I can explain why it is OK to withdraw my trust from someone or something if I feel nervous, uncomfortable or worried.	
4 & 5	I can explain what it means to 'know someone' online and why this might be different from knowing someone in real life.	
4 & 5	I can explain what is meant by 'trusting someone online'. I can explain why this is different to 'liking someone online'.	
4 & 5	I can give examples of how to be respectful to others online.	
4 & 5	I can explain that there are some people I communicate with online who may want to do me or my friends harm. I can recognise that this is not my/our fault.	
5	I can describe strategies for safe and fun experiences in a range of online social environments.	
5	I can make positive contributions and be part of online communities.	
5	I can describe some of the communities in which I am involved in and describe how I collaborate with others positively.	
5	I can show I understand my responsibilities for the well-being of others in my online social group.	

5	I can explain how impulsive and rash communications online may cause problems (e.g. flaming, content produced in online streaming).	
5	I can demonstrate how I would support others (including those who are having difficulties) online.	
5	I can demonstrate ways of reporting problems for both myself and my friends.	

3. Online Reputation	This strand explores the concept of reputation and how others may use online information to make judgements. It offers opportunities to develop strategies to manage personal digital content effectively and capitalise on technology's capacity to create effective positive profiles.

Class	Learning Aim	Possible Resources
KG	I understand that I must not share anything online yet without an adult	
KG & 1	I can identify ways that I can put information on the internet.	
1	I can recognise I need to be careful before I share anything about myself or others online.	
1	I can recognise that information can stay online and could be copied.	
1	I know who I should ask if I am not sure if I should put something online.	
1	I can describe how others can find out information about me by looking online.	
1 & 2	I can explain ways that some of the information about me online could have been created, copied or shared by others.	
2	I can describe what information I should not put online without asking a trusted adult first.	
2	I can explain how information put online about me can last for a long time.	
2 & 3	I know who to talk to if I think someone has made a mistake about putting something online.	
3	I can search for information about myself online.	
4 & 5	I can search for information about an individual online and create a summary report of the information I find.	
5	I can describe ways that information about people online can be used by others to make judgements about an individual.	
5	I can explain how I am developing an online reputation which will allow other people to form an opinion of me.	
5	I can describe some simple ways that help build a positive online reputation.	

4. Online Bullying	This strand explores bullying and other online aggression and how technology impacts those issues. It offers strategies for effective reporting and intervention and considers how bullying and other aggressive behaviour relates to legislation.

Class	Learning Aim	Possible Resources
KG	I know what to do or who could help me if I have been unkind to someone.	
KG, 1 & 2	I know who I can speak to if I or someone else feels bullied.	
1 & 2	I understand how bullying can make someone feel.	
1 & 2	I have ideas how I can help someone who is feeling bullied.	
3	I can describe ways that some people can be unkind online.	
3	I can offer examples of how this can make other people feel.	
3	I can describe how to behave online in ways that do not upset others and can give examples.	
3	I can give examples of bullying behaviour and how it could look online.	
KG & 3	I understand how bullying can make someone feel.	

3	I can talk about how someone can/would get help about being bullied online or offline.	
3	I can describe what bullying is and can describe how people may bully others.	
3	I can describe rules about how to behave online and how I follow them.	
4	I can identify some online technologies where bullying might take place.	
4 & 5	I can describe ways people can be bullied through a range of media (e.g. images, video, text, chat).	

5. Managing Online Information	This strand explores how online information is found, viewed and interpreted. It offers strategies for effective searching, critical evaluation and ethical publishing.

Class	Learning Aim	Possible Resources
KG & 1	I can describe and demonstrate how to get help from a trusted adult or helpline if I find content that makes me feel sad, uncomfortable, worried or frightened.	
KG & 1	I can identify devices I could use to access information on the internet.	
KG & 1	I can give simple examples of how to find information (e.g. search engine, voice activated, searching).	
KG & 1	I can explain how the internet can be used to sell and buy things.	
KG & 1 & 2	I can talk about how I can use the internet to find things out.	
4	I can explain why lots of people sharing the same opinions or beliefs online does not make those opinions or beliefs true.	
4	I can explain what is meant by a 'hoax'. I can explain why I need to think carefully before I forward anything online.	
4	I can use the internet to find things out.	
4	I can use simple keywords in search engines.	
5	I can describe and assess the creative benefits and ethical drawbacks of digital manipulation.	
5	I can describe the laws governing online sexual content.	
5	I am aware that my own personal online activity, history or profile (my 'digital personality') will affect the type of information returned to me in a search or on a social media stream, and intended to influence my beliefs, actions and choices.	
5	I can reflect on and assess the role that digital media plays in my life and give clear examples of where it benefits my lifestyle.	
5	I can assess and manage how and what I contribute to 'big data'.	
5	I can explain why some information I find online may not be honest, accurate or legal.	
5	I can give examples of how organisations representing creative industries challenge and monitor online copyright theft and can outline and evaluate resulting outcomes.	
5	I can apply Creative Commons Licensing to my own work.	
5	I can apply the principles of fair use to my own work and that of others.	
5	I can give examples of where I have done this.	
5	I can explain why copyright on my content may be limited when using social media, website and apps.	
5	I can demonstrate how I can protect my own work from copyright theft.	
5	I can explain the effects of plagiarism within my own work and assess the impact it can have on accrediting achievement.	
5	I can explain the principles of fair use and apply this to case studies.	
5	I understand the concept of software and content licensing.	
5	I understand Creative Commons Licensing.	

5	I can explain how and why I could be targeted for sophisticated information or disinformation intended to influence my beliefs, actions and choices (e.g. gaslighting, information operations).	
5	I can assess how my developing 'digital personality' might affect (focus or limit) the type of information returned to me in a search or on a social media stream.	
5	I can give examples from my own media research of incidences when those laws have been broken.	
5	I can differentiate between genuine news sites and fake (or imitation) news sites with similar web addresses.	
5	I can recognise when and analyse why online content has been designed to deliberately mislead or misinform (e.g. fake news or propaganda).	
5	I can explain ways my own personal online choices, history and profile will be increasingly affecting the type of information returned to me in a search, on a social media stream or through targeted advertising or political messages. I can describe ways of recognising and assessing such targeting.	
5	I can describe the process I use to make ethical choices to ensure my own online content is appropriate, responsible and contributes to a positive online culture. I can give examples of this from my own publishing.	
5	I can explain how search engine rankings are returned and can explain how they can be influenced (e.g. commerce, sponsored results).	
5	I can demonstrate the appropriate routes if I need to report illegal content.	
5	I can refine search phrases with additional functions (e.g. +And, "", not *wildcard).	
5	I can identify and describe some of the laws governing online illegal content and that they may vary from country to country.	
5	I know what to do when this is happening and who might benefit.	
5	I can explain key aspects of copyright law and from my own media research, give examples of where that law has been applied to online content.	
5	I can explain the wider implications of copyright theft on content production and the availability of content (e.g. loss of revenue, emerging artists, new content development).	
5	I can explain how liking, sharing, or forwarding online content can change people's opinions of me (e.g. contribute to my online reputation).	
5	I can explain what is meant by 'being sceptical'. I can give examples of when and why it is important to be 'sceptical'.	
5	I can describe how I can search for information within a wide group of technologies (e.g. social media, image sites, video sites).	
5	I can describe and assess the creative benefits and ethical drawbacks of digital manipulation.	
6	I can use search technologies effectively.	
6	I can use key phrases in search engines.	
6	I can use different search technologies.	
6	I can explain that some people I 'meet online' (e.g. through social media) may be computer programmes pretending to be real people.	
6	I can describe what is meant by 'big data' and 'data analytics' and how political parties, commercial and other organisations use these. I can evaluate the ethics of such use.	

6. Health, Well-being and Lifestyle	This strand explores the impact that technology has on health, well-being and lifestyle. It also includes understanding negative behaviours and issues amplified and sustained by online technologies and the strategies for dealing with them.

Class	Learning Aim	Possible Resources
KG & 1 & 2	I can explain rules to keep us safe when we are using technology both in a beyond the home.	
1 & 2	I can explain how using technology can distract me from other things I might do or should be doing.	
2	I can identify times or situations when I might need to limit the amount of time I use technology. I can suggest strategies to help me limit this time.	
2	I can explain why spending too much time using technology can sometimes have a negative impact on me; I can give some examples of activities where it is easy to spend a lot of time engaged (e.g. games, films, videos).	
3	I can identify rules that help to keep us safe and healthy in and beyond the home when using technology, and I can give some simple examples.	
4	I can explain the importance of self-regulating my use of technology; I can demonstrate the strategies I use to do this (e.g. monitoring my time online, avoiding accidents).	
4 & 5	I can describe some strategies, tips or advice to promote healthy sleep with regards to technology.	
4 & 5	I can describe ways technology can affect healthy sleep and can describe some of the issues.	
4 & 5	I can assess and action different strategies to limit the impact of technology on my health (e.g. night-shift mode, regular breaks, correct posture, sleep, diet and exercise).	
4 & 5	I recognise and can discuss the pressures that technology can place on me and how/when I think I should respond.	
5	I can give some examples of those pressures (e.g. immediate response on social media and messaging apps; always available; invasive; rapid engagement).	
5	I can explain simple guidance for using technology in different environments and settings and I can say how those rules/guides can help me.	

7. Privacy and Security	This strand explores the concept of reputation and how others may use online information to make judgements. It offers opportunities to develop strategies to manage personal digital content effectively and capitalise on technology's capacity to create effective positive profiles.

Class	Learning Aim	Possible Resources
1 & KG	I can explain how many devices in my home could be connected to the internet and can list some of those devices.	
KG & 1	I can identify some simple examples of my personal information (e.g. name, address, birthday, age, location).	
1	I can explain why I should always ask a trusted adult before I share any information about myself online.	
1 & 2	I can describe the people I can trust and can share this with; I can explain why I can trust them.	
1 & 2	I can recognise more detailed examples of information that is personal to me (e.g. where I live, my family's names, where I go to school).	
1 & 2	I can describe how connected devices can collect and share my information with others.	
2	I can explain how passwords can be used to protect information and devices.	
2	I can describe how online information about me could be seen by others.	

2	I can describe and explain some rules for keeping my information private.	
2	I can give reasons why I should only share information with people I choose to and can trust. I can explain that if I am not sure or I feel pressured, I should ask a trusted adult.	
2	I understand and can give reasons why passwords are important.	
3	I can explain what passwords are and can use passwords for my accounts and devices.	
3	I can describe simple strategies for creating and keeping passwords private.	
3	I can explain what a strong password is.	
4	I can describe strategies for keeping my personal information private, depending on context.	
4	I can explain that others online can pretend to be me or other people, including my friends.	
4	I can suggest reasons why they might do this.	
4	I can explain how internet use can be monitored.	

8. Copyright and Ownership	This strand explores the concept of online content. It explores strategies for protecting personal content and crediting the rights of others as well as addressing potential consequences of illegal access, download and distribution.

Class	**Learning Aim**	**Possible Resources**
4	I can explain why copying someone else's work from the internet without permission can cause problems.	
4	I can give examples of what those problems might be.	
4	I can explain why work I create using technology belongs to me.	
4	I can say why it belongs to me (e.g. 'it is my idea' or 'I designed it').	
4	I can save my work so that others know it belongs to me (e.g. filename, name on content).	
4	I know that work I create belongs to me.	
4	I can name my work so that others know it belongs to me.	
4	I can describe why other people's work belongs to them.	
4	I can recognise that content on the internet may belong to other people.	
5	When searching on the internet for content to use, I can explain why I need to consider who owns it and whether I have the right to reuse it, and I can give some simple examples.	
5	I can assess and justify when it is acceptable to use the work of others.	
5	I can give examples of content that is permitted to be reused.	