



Online Safety Policy

(including Online Safety Acceptable Use Agreements)

Reviewed and updated by School Bus:	August 2024
Reviewed and updated by SPT:	March 2025
Lead names updated:	March 2025
Date policy last reviewed and approved:	24 th March 2025
Date of next review:	March 2026
Approved by:	Education Committee

The following have been involved in the developing this policy:

Marcus Cooper - CEO

Karen Cayford – Executive Headteacher, Compliance and Operations

Cathy Longhurst – Executive Headteacher, Behaviour and Safeguarding

Corinna Semon - CFO

Spiral Headteachers

Spiral Computing Subject Leads



Online Safety Policy

(including Online Safety Acceptable Use Agreements)

Contents:

Statement of intent

1. [Legal framework](#)
2. [Roles and responsibilities](#)
3. [Managing online safety](#)
4. [Cyberbullying](#)
5. [Child-on-child sexual abuse and harassment](#)
6. [Grooming and exploitation](#)
7. [Mental health](#)
8. [Online hoaxes and harmful online challenges](#)
9. [Cyber-crime](#)
10. [Online safety training for staff](#)
11. [Online safety and the curriculum](#)
12. [Use of technology in the classroom](#)
13. [Use of smart technology](#)
14. [Educating parents](#)
15. [Internet access](#)
16. [Filtering and monitoring online activity](#)
17. [Network security](#)
18. [Emails](#)
19. [Generative artificial intelligence \(AI\)](#)
20. [Social networking](#)
21. [The school website](#)
22. [Use of devices](#)
23. [Remote learning](#)
24. [Monitoring and review](#)

Appendices

- a. Acceptable Use Agreements
- b. Online Safety Policy Guide – Key Information

Statement of intent

Spiral Partnership Trust (SPT) understands that using online services is an important aspect of raising educational standards, promoting pupil achievement, and enhancing teaching and learning. The use of online services is embedded throughout the school; therefore, there are a number of controls in place to ensure the safety of pupils and staff.

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

Content: Being exposed to illegal, inappropriate or harmful material, e.g. pornography, fake news, self-harm and suicide, and discriminatory or extremist views.

Contact: Being subjected to harmful online interaction with other users, e.g. peer pressure, commercial advertising, and adults posing as children or young adults with the intention to groom or exploit children.

Conduct: Personal online behaviour that increases the likelihood of, or causes, harm, e.g. sending and receiving explicit messages, and cyberbullying.

Commerce: Risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

The measures implemented to protect pupils and staff revolve around these areas of risk and this policy aims to ensure appropriate and safe use of the internet and other digital technology devices by all pupils and staff.

1. Legal framework

This policy has due regard to all relevant legislation and guidance including, but not limited to, the following:

- Voyeurism (Offences) Act 2019
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- DfE (2024) 'Filtering and monitoring standards for schools and colleges'
- DfE (2021) 'Harmful online challenges and online hoaxes'
- DfE (2024) 'Keeping children safe in education 2024'
- DfE (2023) 'Teaching online safety in school'
- DfE (2022) 'Searching, screening and confiscation'
- DfE (2023) 'Generative artificial intelligence in education'
- Department for Science, Innovation and Technology and UK Council for Internet Safety (2024) 'Sharing nudes and semi-nudes: advice for education settings working with children and young people'
- UK Council for Child Internet Safety (2020) 'Education for a Connected World – 2020 edition'
- National Cyber Security Centre (2020) 'Small Business Guide: Cyber Security'

This policy operates in conjunction with the following school policies:

- Allegations of Abuse Against Staff Policy
- Acceptable Use Agreements
- Anti-Bullying Policy
- Behaviour Policy
- Confidentiality Agreement
- Cyber-security Policy
- Cyber Response and Recovery Plan
- Child Protection Policy
- Device User Agreement
- Disciplinary Policy and Procedure
- GDPR Policy
- Privacy Notices
- Staff Code of Conduct
- Whistleblowing Policy

2. Roles and responsibilities

The Spiral Partnership Trust Board and its nominated committee has ultimate responsibility to ensure that appropriate online safety policy and practice is embedded and monitored throughout the Trust. This is delegated as follows:

Fleetville Infant School – Jen Gardner
Fleetville Junior School – Clare Whitehouse
Forres Primary Academy – Gavin Douglas
Mount Pleasant Lane School – Alex Lindley/Jennifer Bradshaw
Mandeville Primary School – Cathy Longhurst
Springmead Primary School – Karen Cayford/Hannah Clarke
Spiral Partnership Trust – Marcus Cooper

All breaches of this policy must be reported to the school's Headteacher/Head of School and recorded in the school's online safety breaches record.

All breaches of this policy that may have put a child at risk must also be reported to the DSP.

The Spiral Partnership Trust Board is responsible for:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- Ensuring the Designated Safeguarding Lead's (DSL's) remit covers online safety.
- Reviewing this policy on an annual basis.
- Ensuring their own knowledge of online safety issues is up-to-date.
- Ensuring all staff undergo safeguarding and child protection training, including online safety, at induction and at regular intervals.
- Ensuring that there are appropriate filtering and monitoring systems in place.
- Ensuring that the effectiveness of filtering and monitoring systems is reviewed at least annually in liaison with ICT staff and service providers.
- Ensuring that school and Trust leadership and other relevant staff have an awareness and understanding of the filtering and monitoring provisions in place, and manage them effectively and know how to escalate concerns when identified.
- Ensuring that all relevant school policies have an effective approach to planning for, and responding to, online challenges and hoaxes embedded within them.

The Headteacher/Head of School will be responsible for:

- Ensuring that online safety is a running and interrelated theme throughout the school's policies and procedures, including in those related to the curriculum, teacher training and safeguarding.
- Supporting the DSL and deputy DSLs by ensuring they have enough time and resources to carry out their responsibilities in relation to online safety.
- Ensuring staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and safeguarding training.
- Ensuring online safety practices are audited and evaluated.
- Organising engagement with parents to keep them up-to-date with current online safety issues and how the school is keeping pupils safe.

The DSL will be responsible for:

- Taking the lead responsibility for online safety in the school.
- Undertaking training so they understand the risks associated with online safety and can recognise additional risks that pupils with SEND face online.
- Ensuring the internet, mobile and digital technologies are used effectively and safely for their intended purpose and in ways that will not infringe legal requirements or pose unnecessary risks.
- Liaising with relevant members of staff on online safety matters, e.g. the SENCO and ICT technicians when required.
- Ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented.
- Ensuring safeguarding is considered in the school's approach to remote learning.
- Following the SPT procedure for reporting online safety incidents and inappropriate internet use, both by pupils and staff, and ensuring all members of the school community understand this procedure.
- Understanding the filtering and monitoring processes in place at the school.

- Ensuring that all safeguarding training given to staff includes an understanding of the expectations, roles and responsibilities in relation to filtering and monitoring systems at the school.
- Maintaining detailed, secure and accurate written records of reported online safety concerns as well as the decisions and whether or not referrals have been made.
- Understanding the purpose of record keeping.
- Monitoring online safety incidents to identify trends and any gaps in the school's provision, and using this data to update the school's procedures.
- Reporting to their Local School Committee about online safety on a regular basis.

ICT Service Providers will be responsible for:

- Providing technical support in the development and implementation of the school's online safety policies and procedures.
- Implementing appropriate security measures as directed by the headteacher.
- Ensuring that the school's filtering and monitoring systems are updated as appropriate.

All staff members will be responsible for:

- Taking responsibility for the security of ICT systems and electronic data they use or have access to.
- Modelling good online behaviours.
- Maintaining a professional level of conduct in their personal use of technology.
- Having an awareness of online safety issues.
- Ensuring they are familiar with, and understand, the indicators that pupils may be unsafe online.
- Reporting concerns in line with the SPT reporting procedure.
- Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum.

Pupils will be responsible for:

- Adhering to the Acceptable Use Agreement and other relevant policies.
- Seeking help from school staff if they are concerned about something they or a peer have experienced online.
- Using technology and online platforms in line with the expectations of this policy in all areas of life outside of school.
- Reporting online safety incidents and concerns in line with the procedures within this policy.

3. Managing online safety

All staff will be aware that technology is a significant component in many safeguarding and wellbeing issues affecting children and young people, particularly owing to the rise of social media and the increased prevalence of children using the internet.

The DSL has overall responsibility for a school's approach to online safety, with support from deputy DSLs and the Headteacher/Head of School where appropriate, and will ensure that there are strong processes in place to handle any concerns about pupils' safety online. The DSL should liaise with the police or children's social care services for support responding to harmful online sexual behaviour.

The importance of online safety is integrated across all school operations in the following ways:

- Annual online safety training for staff and Committee Members.

- Staff receive regular email updates regarding online safety information and any changes to online safety guidance or legislation.
- Online safety is integrated into learning throughout the curriculum.
- Assemblies are conducted termly on the topic of remaining safe online.

Handling online safety concerns

Any disclosures made by pupils to staff members about online abuse, harassment or exploitation, whether they are the victim or disclosing on behalf of another child, will be handled in line with the Child Protection Policy.

Concerns regarding a staff member's online behaviour are reported to the Headteacher/Head of School, who decides on the best course of action in line with the relevant policies. If the concern is about the Headteacher/Head of School, it is reported to the chair of the Local School Committee.

Concerns regarding a pupil's online behaviour are reported to the DSL, who investigates concerns with relevant staff members, e.g. the Headteacher/Head of School and ICT technicians, and manages concerns in accordance with relevant policies depending on their nature, e.g. the Behaviour Policy and Child Protection Policy.

Where there is a concern that illegal activity has taken place, the Headteacher/Head of School contacts the police.

Spiral Partnership Trust avoids unnecessarily criminalising pupils, e.g. calling the police, where criminal behaviour is thought to be inadvertent and as a result of ignorance or normal developmental curiosity, e.g. a pupil has taken and distributed indecent imagery of themselves. The DSL will decide in which cases this response is appropriate and will manage such cases in line with the Child Protection Policy.

All online safety incidents and the school's response are recorded by the DSL.

4. Cyberbullying

Cyberbullying can include, but is not limited to, the following:

- Threatening, intimidating or upsetting text messages.
- Threatening or embarrassing pictures and video clips sent via mobile phone cameras.
- Silent or abusive phone calls or using the victim's phone to harass others, to make them think the victim is responsible.
- Threatening or bullying emails, possibly sent using a pseudonym or someone else's name.
- Unpleasant messages sent via instant messaging.
- Unpleasant or defamatory information posted to blogs, personal websites and social networking sites, e.g. Instagram.
- Abuse between young people in intimate relationships online i.e. teenage relationship abuse.
- Discriminatory bullying online i.e. homophobia, racism, misogyny/misandry.

The school will be aware that certain pupils can be more at risk of abuse and/or bullying online, such as pupils with SEND.

Cyberbullying against pupils or staff is not tolerated under any circumstances. Incidents of cyberbullying are dealt with quickly and effectively wherever they occur in line with a school's Anti-bullying Policy.

5. Child-on-child sexual abuse and harassment

All staff will be aware of the indicators of abuse, neglect and exploitation and understand where the risk of such harms can occur online. Staff will understand that this can occur both in and outside of school, off and online, and will remain aware that pupils are less likely to report concerning online sexual behaviours, particularly if they are using websites that they know adults will consider to be inappropriate for their age.

The following are examples of online harmful sexual behaviour of which staff will be expected to be aware:

- Threatening, facilitating or encouraging sexual violence.
- Upskirting, i.e. taking a picture underneath a person's clothing without consent and with the intention of viewing their genitals, breasts or buttocks.
- Sexualised online bullying, e.g. sexual jokes or taunts.
- Unwanted and unsolicited sexual comments and messages.
- Consensual or non-consensual sharing of sexualised imagery.

All staff will be aware of and promote a zero-tolerance approach to sexually harassing or abusive behaviour, and any attempts to pass such behaviour off as trivial or harmless. Staff will be aware that allowing such behaviour could lead to a school culture that normalises abuse and leads to pupils becoming less likely to report such conduct.

Staff will be aware that creating, possessing, and distributing indecent imagery of other children, i.e. individuals under the age of 18, is a criminal offence, even where the imagery is created, possessed, and distributed with the permission of the child depicted, or by the child themselves. All occurrences will be reported to the relevant authorities.

All concerns regarding online child-on-child sexual abuse and harassment will be investigated, regardless of whether the incident took place on the school premises or using school-owned equipment. Concerns regarding online child-on-child abuse will be reported to the DSL, who will investigate the matter in line with the Child Protection Policy.

6. Grooming and exploitation

Grooming is defined as the situation whereby an adult builds a relationship, trust and emotional connection with a child or other adult with the intention of manipulating, exploiting and/or abusing them.

Staff will be aware that grooming often takes place online and that pupils who are being groomed are commonly unlikely to report this behaviour for many reasons, e.g. the pupil may have been manipulated into feeling a strong bond with their groomer and may have feelings of loyalty, admiration, or love, as well as fear, distress and confusion.

Due to the fact pupils are less likely to report grooming than other online offences, it is particularly important that staff understand the indicators of this type of abuse. The DSL will ensure that online safety training covers online abuse, the importance of looking for signs of grooming, and what the signs of online grooming are, including:

- Being secretive about how they are spending their time online.
- Having an older boyfriend or girlfriend, usually one that does not attend the school and whom their close friends have not met.

- Having money or new possessions, e.g. clothes and technological devices, that they cannot or will not explain.

Child sexual exploitation (CSE) and child criminal exploitation (CCE)

Although CSE often involves physical sexual abuse or violence, online elements may be prevalent, e.g. sexual coercion and encouraging children to behave in sexually inappropriate ways through the internet. In some cases, a pupil may be groomed online to become involved in a wider network of exploitation, e.g. the production of child pornography or forced child prostitution and sexual trafficking.

CCE is a form of exploitation in which children are forced or manipulated into committing crimes for the benefit of their abuser, e.g. drug transporting, shoplifting and serious violence. While these crimes often take place in person, it is increasingly common for children to be groomed and manipulated into participating through the internet.

Where staff have any concerns about pupils with relation to CSE or CCE, they will bring these concerns to the DSL without delay, who will manage the situation in line with the Child Protection Policy.

Radicalisation

Radicalisation is the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups. This process can occur through direct recruitment, e.g. individuals in extremist groups identifying, targeting and contacting young people with the intention of involving them in terrorist activity, or by exposure to violent ideological propaganda. Children and adults who are targets for radicalisation are likely to be groomed by extremists online to the extent that they believe the extremist has their best interests at heart, making them more likely to adopt the same radical ideology.

Staff members will be aware of the factors which can place certain pupils or staff at increased vulnerability to radicalisation, as outlined in the Prevent Duty Policy. Staff will be expected to exercise vigilance towards any pupils or colleagues displaying indicators that they have been, or are being, radicalised. Where staff have a concern about radicalisation, they will report this to the DSL without delay, who will handle the situation in line with the Child Protection Policy.

7. Mental health

Staff will be aware that online activity both in and outside of school can have a substantial impact on a pupil's mental state, both positively and negatively. The DSL will ensure that training is available to help ensure that staff members understand popular social media sites and terminology, the ways in which social media and the internet in general can impact mental health, and the indicators that a pupil is suffering from challenges in their mental health. Concerns about the mental health of a pupil will be dealt with in line with Child Protection Policy.

8. Online hoaxes and harmful online challenges

For the purposes of this policy, an "online hoax" is defined as a deliberate lie designed to seem truthful, normally one that is intended to scaremonger or to distress individuals who come across it, spread on online social media platforms.

For the purposes of this policy, "harmful online challenges" refers to challenges that are targeted at young people and generally involve users recording themselves participating in an online challenge, distributing the video through social media channels and daring others to do the same. Although many

online challenges are harmless, an online challenge becomes harmful when it could potentially put the participant at risk of harm, either directly as a result of partaking in the challenge itself or indirectly as a result of the distribution of the video online – the latter will usually depend on the age of the pupil and the way in which they are depicted in the video.

Where staff suspect there may be a harmful online challenge or online hoax circulating amongst pupils in the school, they will report this to the DSL immediately.

The DSL will conduct a case-by-case assessment for any harmful online content brought to their attention, establishing the scale and nature of the possible risk to pupils, and whether the risk is one that is localised to the school or the local area, or whether it extends more widely across the country. Where the harmful content is prevalent mainly in the local area, the DSL will consult with the LA about whether quick local action can prevent the hoax or challenge from spreading more widely.

Prior to deciding how to respond to a harmful online challenge or hoax, the DSL and the Headteacher/Head of School will decide whether each proposed response is:

- In line with any advice received from a known, reliable source, e.g. the UK Safer Internet Centre, when fact-checking the risk of online challenges or hoaxes.
- Careful to avoid needlessly scaring or distressing pupils.
- Not inadvertently encouraging pupils to view the hoax or challenge where they would not have otherwise come across it, e.g. where content is explained to younger pupils but is almost exclusively being shared amongst older pupils.
- Proportional to the actual or perceived risk.
- Helpful to the pupils who are, or are perceived to be, at risk.
- Appropriate for the relevant pupils' age and developmental stage.
- Supportive.
- In line with the Child Protection Policy.

Where the DSL's assessment finds an online challenge to be putting pupils at risk of harm, they will ensure that the challenge is directly addressed to the relevant pupils, e.g. those within a particular age range that is directly affected or individual pupils at risk where appropriate.

The DSL and Headteacher/Head of School will only implement a school-wide approach to highlighting potential harms of a hoax or challenge when the risk of needlessly increasing pupils' exposure to the risk is considered and mitigated as far as possible.

9. Cyber-crime

Cyber-crime is criminal activity committed using computers and/or the internet. There are two key categories of cyber-crime:

- **Cyber-enabled** – these crimes can be carried out offline; however, are made easier and can be conducted at higher scales and speeds online, e.g. fraud, purchasing and selling of illegal drugs, and sexual abuse and exploitation.
- **Cyber-dependent** – these crimes can only be carried out online or by using a computer, e.g. making, supplying or obtaining malware, illegal hacking, and 'booting', which means overwhelming a network, computer or website with internet traffic to render it unavailable.

The DSL and Headteacher/Head of School will ensure that pupils are taught, throughout the curriculum, how to use technology safely, responsibly and lawfully. In addition, the school will implement a cyber awareness plan for pupils and staff to ensure that they understand the basics of cyber security and protecting themselves from cybercrime.

The school will implement its cyber security strategy in line with the DfE's 'Cyber security standards for schools and colleges'.

10. Online safety training for staff

The DSL will ensure that all safeguarding training given to staff includes elements of online safety, including how the internet can facilitate abuse and exploitation, and understanding the expectations, roles and responsibilities relating to filtering and monitoring systems. All staff will be made aware that pupils are at risk of abuse, by their peers and by adults, online as well as in person, and that, often, abuse will take place concurrently via online channels and in daily life.

11. Online safety and the curriculum

Online safety is embedded throughout the curriculum; however, it is particularly addressed in the following subjects:

- Relationships and health education
- PSHE
- Computing

Online safety teaching is always appropriate to pupils' ages and developmental stages.

Pupils are taught the underpinning knowledge and behaviours that can help them to navigate the online world safely and confidently regardless of the device, platform or app they are using. The underpinning knowledge and behaviours pupils learn through the curriculum include the following:

- How to evaluate what they see online
- How to recognise techniques used for persuasion
- Acceptable and unacceptable online behaviour
- How to identify online risks
- How and when to seek support
- Knowledge and behaviours that are covered in the government's online media literacy strategy

The online risks pupils may face are always considered when developing the curriculum. The DSL will be involved with the development of the school's online safety curriculum. Pupils will be consulted on the online safety curriculum, where appropriate, due to their unique knowledge of the kinds of websites they and their peers frequent and the kinds of behaviours in which they engage online.

Relevant members of staff, e.g. the SENCO and designated teacher for LAC, will work together to ensure the curriculum is tailored so that pupils who may be more vulnerable to online harms, e.g. pupils with SEND and LAC, receive the information and support they need. The school will also endeavour to take a more personalised or contextualised approach to teaching about online safety for more susceptible children, and in response to instances of harmful online behaviour from pupils.

Class teachers will review external resources prior to using them for the online safety curriculum, to ensure they are appropriate for the cohort of pupils.

External visitors may be invited into school to help with the delivery of certain aspects of the online safety curriculum. The Headteacher/Head of School and DSL will decide when it is appropriate to invite external groups into school and ensure the visitors selected are appropriate.

Before conducting a lesson or activity on online safety, the class teacher and DSL will consider the topic that is being covered and the potential that pupils in the class have suffered or may be suffering from online abuse or harm in this way. Where necessary, the DSL will advise the staff member on how to best support any pupil who may be especially impacted by a lesson or activity. Lessons and activities will be planned carefully so they do not draw attention to a pupil who is being or has been abused or harmed online, to avoid publicising the abuse.

During an online safety lesson or activity, the class teacher will ensure a safe environment is maintained in which pupils feel comfortable to say what they feel and ask questions, and are not worried about getting into trouble or being judged.

If a staff member is concerned about anything pupils raises or discloses during online safety lessons and activities, they will make a report in line with the Child Protection Policy.

12. Use of technology in the classroom

A wide range of technology will be used during lessons, including the following:

- Computers/desktops
- Laptops/Chromebooks
- Tablets
- Email (internal only)
- Cameras

Prior to using any websites, tools, apps or other online platforms in the classroom, or recommending that pupils use these platforms at home, the class teacher will review and evaluate the resource. Class teachers will ensure that any internet-derived materials are used in line with copyright law.

Pupils will be supervised when using online materials during lesson time – this supervision is suitable to their age and ability.

13. Use of smart technology

Trust schools recognises that the use of smart technology can have educational benefits, there are also a variety of associated risks which the schools will ensure it manages. Key Stage 2 pupils will be educated on the acceptable and appropriate use of personal devices and will use technology in line with the Online Safety Acceptable Use Agreement for Key Stage 2 Pupils (see Appendix A).

Trust schools recognise that pupils' unlimited and unrestricted access to the internet via mobile phone networks means that some pupils may use the internet in a way which breaches the school's acceptable use of ICT agreement for pupils.

Inappropriate use of smart technology may include:

- Using mobile and smart technology to harass, bully, troll or intimidate peers.
- Sharing indecent images, both consensually and non-consensually.
- Viewing and sharing pornography and other harmful content.

Pupils will not be permitted to use smart devices or any other personal technology whilst on school premises. Where there is a significant problem with the misuse of smart technology among pupils, the school will discipline those involved in line with the school's Behaviour Policy.

Trust school will hold assemblies, where appropriate, which address any specific concerns related to the misuse of smart technology and outline the importance of using smart technology in an appropriate manner.

Trust schools will seek to ensure that it is kept up to date with the latest devices, platforms, apps, trends and related threats.

Trust schools will consider the 4Cs (content, contact, conduct and commerce) when educating pupils about the risks involved with the inappropriate use of smart technology and enforcing the appropriate disciplinary measures.

Staff and governance members, peripatetic teachers, coaches and supply teachers will use all smart technology and personal technology in line with the relevant acceptable use agreement (see Appendix A).

14. Educating parents

Trust school will work in partnership with parents to ensure pupils stay safe online at school and at home. Parents will be provided with information about the school's approach to online safety and their role in protecting their children. Parents will be sent a copy of the Online Safety Acceptable Use Agreement – Key Stage 2 Pupils (see Appendix A) at the beginning of each academic year and are encouraged to go through this with their child to ensure their child understands the document and the implications of not following it. They will also be sent the Online Safety Policy Guide – Key Information (see Appendix B).

Parents will be made aware of the various ways in which their children may be at risk online, including, but not limited to:

- Child sexual abuse, including grooming.
- Exposure to radicalising content.
- Sharing of indecent imagery of pupils, e.g. sexting.
- Cyberbullying.
- Exposure to age-inappropriate content, e.g. pornography.
- Exposure to harmful content, e.g. content that encourages self-destructive behaviour.

Parents will be informed of the ways in which they can prevent their child from accessing harmful content at home, e.g. by implementing parental controls to block age-inappropriate content. This will be done in a variety of ways, for example:

- Parents' evenings
- Twilight training sessions
- Newsletters
- Online resources

15. Internet access

Staff and other members of the Spiral Partnership Trust community will only be granted access to a school's internet network once they have read and signed the Acceptable Use Agreement (see Appendix A) and have completed the mandatory cyber security training.

Only Trust approved devices will be allowed access to the Trust's internet network(s). Personal mobile phones will not be allowed access unless agreed by the CEO. Guests will be issued a time-restricted

voucher and will be required to agree to the terms and conditions of use as set out by Spiral Partnership Trust.

16. Filtering and monitoring online activity

The Spiral Partnership Trust board will ensure the Trust's ICT networks have appropriate filters and monitoring systems in place and that it is meeting the DfE's '[Filtering and monitoring standards for schools and colleges](#)'. The Spiral Partnership Trust board will ensure 'over blocking' does not lead to unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.

The Headteacher/Head of School and ICT technicians will undertake a risk assessment to determine what filtering and monitoring systems are required. The filtering and monitoring systems the Trust and schools will be appropriate to the needs of staff and pupils. ICT technicians will undertake checks on the filtering and monitoring systems to ensure they are effective and appropriate. The Executive Head – Compliance and Operations will review filtering systems in line with the requirements of Keeping Children Safe in Education.

Requests regarding making changes to the filtering system will be directed to the Executive Head – Compliance and Operations. Any changes made to the system will be recorded by the Executive Head – Compliance and Operations. Reports of inappropriate websites or materials will be made via the Croft help.it@croftmsp.com ticket system who will then investigate the matter and make any necessary changes.

Deliberate breaches of the filtering system will be reported to the Executive Head – Compliance and Operations, who will escalate the matter appropriately. If a pupil has deliberately breached the filtering system, they will be disciplined in line with the Behaviour Policy. If a member of staff has deliberately breached the filtering system, they will be disciplined in line with the Disciplinary Policy.

If material that is believed to be illegal is accessed, inadvertently or deliberately, this material will be reported to the appropriate agency immediately, e.g. the Internet Watch Foundation (IWF), CEOP and/or the police.

All Trust networks and school-owned devices will be appropriately monitored. All users of the network and school-owned devices will be informed about how and why they are monitored. Concerns identified through monitoring will be reported to the DSL who will manage the situation in line with the Child Protection Policy.

17. Network security

Technical security features, such as anti-virus software, will be kept up-to-date and managed by ICT technicians. Firewalls will be switched on at all times. ICT technicians will review the firewalls on a continual basis to ensure they are running correctly, and to carry out any required updates.

Staff and pupils are advised not to download unapproved software or open unfamiliar email attachments, and will be expected to report all malware and virus attacks to ICT technicians.

All members of staff will have their own unique usernames and private passwords to access the school's systems. Pupils are provided with their own unique username and private passwords at the time when it is age-appropriate to do so. Staff members and pupils will be responsible for keeping their passwords private. Passwords will have a minimum and maximum length and require a mixture of letters, numbers and symbols to ensure they are as secure as possible. Network passwords will expire after 6 months, after which users will be required to change them.

Users will not be permitted to share their login details with others and will not be allowed to log in as another user at any time. If a user is found to be sharing their login details or otherwise mistreating the password system, the Headteacher/Head of School will be informed and will decide the necessary action to take.

Users are required to lock access to devices and systems when they are not in use.

Staff will only access remote systems via the approved Trust systems using Trust-owned devices.

18. Emails

Access to and the use of emails will be managed in line with the Data Protection Policy and Acceptable Use Agreement.

Staff, governance members and pupils will be given approved Trust or school email accounts and will only be able to use these accounts when doing Trust or school-related work outside of school hours. Prior to being authorised to use the email system, staff and pupils must agree to and sign the Acceptable Use Agreement. Personal email accounts will not be permitted to be used on the school site. Any email that contains sensitive or personal information will only be sent using secure and/or encrypted email.

All user of email will be required to block spam and junk mail. The schools monitoring systems can detect inappropriate links, malware and profanity within emails – staff and pupils will be made aware of this. Chain letters, spam and all other emails from unknown sources will be deleted without being opened. Training will be provided to explain what a phishing email and other malicious emails might look like.

Any cyber-attacks initiated through emails will be managed in line with the Critical Incident Framework.

19. Generative artificial intelligence (AI)

Trust schools will take steps to prepare pupils for changing and emerging technologies, e.g. generative AI and how to use them safely and appropriately with consideration given to pupils' age.

Trust schools will ensure its IT system includes appropriate filtering and monitoring systems to limit pupil's ability to access or create harmful or inappropriate content through generative AI.

Trust schools will ensure that pupils are not accessing or creating harmful or inappropriate content, including through generative AI.

Staff and governance members will only use AI in line with the Trust's Artificial Intelligence Policy.

20. Social networking

The use of social media by staff and pupils will be managed in line with the Trust's Code of Conduct.

21. Trust Websites

The CEO and the Headteachers/Heads of School will be responsible for the overall content of the Trust and school websites. They will ensure the content is appropriate, accurate, up-to-date and meets government and legal requirements.

22. Use of devices, including personal

Where necessary, staff members and pupils will be issued with Trust or school-owned devices to assist with their work. Requirements around the use of Trust or school-owned devices can be found in the Acceptable Use Policies (see Appendix A).

The school or Trust allows staff, including temporary and peripatetic staff, and visitors to use personal mobile phones and devices only in designated areas (see below) and never in the presence of pupils. Under no circumstance does the school or Trust allow a member of staff to contact a pupil or parent/carers using their personal device.

Spiral School	Rooms allowed
Fleetville Infant School	Staff Room/PPA Room/Offices
Fleetville Junior School	Staff Room/PPA Room/Offices
Forres Primary Academy	Staff Room/PPA Room/Offices
Mount Pleasant Lane School	Staff Room/PPA Room/Offices
Mandeville Primary School	Staff Room/PPA Room/Offices
Springmead Primary School	Staff Room/PPA Room/Offices
Spiral Trust	Trust Offices
Spiral Faces	Staff Room/Offices
DSPL7	Offices

Parents/carers may only use personal mobile phones and devices in designated areas unless otherwise informed, e.g. for specific events and activities. Under no circumstance should images be taken at any time on Trust premises or on off-site school events and activities of anyone other than their own child, unless there is a pre-specified permission from the school's Headteacher/Head of School. When a parent/carers is on school premises but not in a designated area, their phone/s must be switched off and out of sight.

Pupils are allowed to bring personal mobile devices/phones to school but must not use them whilst on the school premises or for personal purposes within lesson time. Each school will have a system by which student phones are stored securely during the school day. Under no circumstance should pupils use their personal mobile devices/phones to take images of:

- any other pupil unless they and their parents have given agreement in advance
- any member of staff
- any buildings, rooms or outside areas within the school premises

The school is not responsible for the loss, damage or theft of any personal mobile device that is brought into school. Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

23. Access to sensitive information and storage of images

GDPR requires all school data to be safe. It is permissible to use personal devices to access school email but only if the device is locked via a passcode, fingerprint or face recognition system and via the Microsoft Outlook app. Any staff member who loses their device must inform the IT Technicians via the help.it@croftmsp.com ticket system to enable blocking of access to emails. Emails must not be accessible by anyone who is not an employee of Spiral Partnership Trust. If this is the case, then a second two-factor authentication method must be used to restrict access to emails. No documents

or information is to be downloaded onto a personal device unless it is owned by the Spiral Partnership Trust.

Access to the MIS and CPOMs is only allowed via two-factor authentication whilst off-site. These systems must not be accessible by anyone who is not an employee of Spiral Partnership Trust along with any other platform that contains details of staff or pupils.

Photographs and videos provide valuable evidence of pupils' achievement and progress in a variety of contexts and can be used to celebrate the work of the school. In line with GDPR they are used only with the written consent of parents/carers which is secured in the first instance on a child's entry to the school. Records are kept on file and consent can be changed by parents/carers at any time. (See GDPR policy for greater clarification).

Photographs and images of pupils are only stored on a school's agreed secure networks which include some cloud-based services. Rights of access to stored images are restricted to approved staff as determined by the school's Headteacher/Head of School. Staff and pupils may have temporary access to photographs taken during a class session, but these will be transferred/deleted promptly.

Parents/carers should note that there may be some children who are at risk and must not have their image put online and others who do not want their image online. For these reasons parents/carers must follow the school's Acceptable Use Agreement and refrain from taking or posting online photographs of any member of the school community, other than their own child/ren.

Staff and other professionals working with pupils, must only use school equipment to record images of pupils whether on or off site. Permission to use images of all staff who work at the school is sought on induction and a written record is located in the personnel file.

24. Monitoring and review

Trust schools recognise that the online world is constantly changing; therefore, the DSL, ICT technicians and the Executive Headteacher – Compliance and Operations conducts regular light-touch reviews of this policy to evaluate its effectiveness.

Any changes made to this policy are communicated to all members of the school community.

APPENDIX A

Name of school/Trust team	
Online Safety Acceptable Use Agreement for Staff and Governance	
Online Safety Lead	
Designated Safeguarding Lead (DSP)	

ICT (including data) and the related technologies such as email, the internet and mobile devices (including personal) are an expected part of our daily working life in school. This agreement is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with Marcus Cooper, CEO.

- I will only use the Trust or school's email / Internet / Learning Platform and any related technologies for professional purposes or for uses deemed acceptable by the Head or Trust Board;
- I will comply with the ICT system security and not disclose any personal passwords or those provided to me by the school or Trust;
- I will use two-factor authentication on all systems as dictated by the Trust, including Arbor and CPOMS whilst off-site;
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role;
- I will refrain from inappropriate online sexual harassment activities, including via personal devices;
- I will not give out my own personal details, such as mobile phone number, personal email address, personal social media accounts, or any other social media link, to pupils. This includes devices provided by Spiral Trust as part of my work;
- I will only use the approved, secure email system(s) and applications for any school business;
- I will ensure that personal data (such as data held on MIS software) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head/Head of School. Personal or sensitive data taken off site must be encrypted, e.g. on a password secured laptop;
- I will not upload any personal data relating to students or staff onto an external or cloud-based system without the permission of the Headteacher/Head of School or CEO;
- I will not install any hardware or software without permission, including mobile applications;
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory;
- Images of pupils and/or staff will only be taken on school/Trust devices, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member;
- Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher/Head of School;
- I will support the school approach to online safety and not upload or add any images, video, sounds or text linked to or associated with the school or its community';
- I understand that all my use of the internet and other related technologies can be monitored and logged and can be made available, on request, to my Headteacher/Head of School or the CEO;
- I will respect copyright and intellectual property rights;

- I will ensure that my online activity, both in school and outside school, will not bring the school, my professional reputation, or that of others, into disrepute;
- I will support and promote the school's online safety policy and help pupils to be safe and responsible in their use of ICT and related technologies;
- I will not use personal electronic devices (including smart watches) in public areas of the school whilst pupils are on site, except in the areas outlined within this policy;
- I understand this forms part of the terms and conditions set out in my contract of employment.

User signature

I agree to follow this Acceptable Use Agreement and to support the safe and secure use of ICT throughout the school.

Signature
 Full Name
 (printed)
 Job Title
 Date

Name of school	
Online Safety Acceptable Use Agreement for Peripatetic teachers, coaches and supply teachers.	
Online Safety Lead	
Designated Safeguarding Lead (DSP)	

This agreement forms part of your professional and safeguarding responsibility in the school. You must read and sign this agreement. This will be kept on record and you should retain your own copy for reference.

Internet, mobile and digital technologies are part of our daily working life and this agreement is designed to ensure that all staff and governors are aware of their responsibilities in relation to their use. You are expected to adhere to this agreement. Any concerns or clarification should be discussed with the schools Headteacher or Online Safety Leader. Breaches will be investigated, recorded and, where appropriate, disciplinary procedures will apply and police involvement will be sought.

The school's online safety policy will provide further detailed information as required.

Internet Access

I will not access or attempt to access any sites that contain any of the following: child abuse; pornography; discrimination of any kind; promotion of prejudice against any group; promotion of illegal acts; any other information which may be illegal or offensive. Inadvertent access on school equipment must be treated as an online safety incident, reported to the online safety lead and/or DSP and an incident report completed.

Online conduct

I will ensure that my online activity, both in and outside school, will not bring the school, my professional reputation, or that of others, into disrepute.

I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory. Exceptionally, use of controversial material as part of the curriculum should be planned and approved on every occasion (see policy).

I will report any accidental access to or receipt of inappropriate materials or filtering breach to the schools Online Safety Lead or Headteacher/Head of School.

I understand that all my use of the Trust internet systems and other related technologies can be traced and monitored and, should it be required, must be made available to the CEO or Headteacher/Head of School as required.

I will not give out my personal contact and online account information such as phone numbers, email address, and social media account details to pupils and/or parents/carers.

Should I need to share my professional details, such as mobile phone number or email address, with parent/carers, this must be agreed in advance as an acceptable approach with the school's Headteacher/Head of School.

Social networking

I understand the need to separate my professional role from my private friendships; in my professional capacity I will not become 'friends' with parents/carers or pupils on social networks. Where my school role is my only connection to an individual, private online contact is unacceptable with parents/carers or pupils.

Information can be shared with parents/carers through an organisational social network site/page e.g. on Facebook or Twitter, but never through a personal account or site. In my professional role in the school, I will never engage in 1:1 exchanges with pupils or parent/carers on personal social network sites.

My private account postings will never undermine or disparage the school, its staff, governors, parents/carers or pupils. Privileged information known as a result of my work in the school must remain confidential.

I will not upload any material about or references to the school or its community on my personal social networks.

Passwords

I must clarify what access I may have to the internet and/or school systems. If I have access of any kind, I understand that there is no occasion when a password should be shared with a pupil or anyone who is not a staff member.

Data protection

I will follow all requirements for data protection explained to me by the school. These include:

- I must consult with the school before making any recordings, photographs and videos. Once agreed, these must be made on a school device.
- I understand that there are strict controls and requirements regarding the collection and use of personal data. I will follow all requirements regarding GDPR.

Images and videos

I will only upload images or videos of staff, pupils or parents/carers onto school approved sites where specific permission has been granted.

I will not take images, sound recordings or videos of tuition or wider school activities on any personal device. School devices can be used for this purpose or, in the case of 1:1 tuition, pupil or parent/carer devices can be used, with parent/carer agreement.

Internet, mobile and digital technologies provide helpful recording functions but these cannot be made on a teacher's personal device. Recordings can be made with the child's and parent/carer's agreement on a school device, an organisational device approved by the Headteacher/Head of School/DSP, or a young person's or parent/carer's own device.

Use of Email

I will only use my professional email address for all school business. All such correspondence should be kept professional and is open to Subject Access Requests under the Freedom of Information Act. I will not use my professional email addresses for personal matters in relation to school or Trust staff.

Use of personal devices

I understand that when working in the school I should at no time put myself in a position where a

safeguarding allegation can be made against me as a result of my use of personal devices. I understand that the use of personal devices in school is at the discretion of the Headteacher/Head of School.

I will only use approved personal devices in designated areas and never in front of pupils. This therefore precludes use of specialist apps on personal devices. A school device could be used to access specialist apps that support pupil learning.

Additional hardware/software

I will not install any hardware or software on school equipment without permission of the Headteacher/Head of School.

Promoting online safety

I understand that online safety is part of my responsibility and I will promote positive online safety messages at all times, including when setting homework, rehearsal or skill practice or when providing pastoral support.

I understand that it is my duty to support a whole school safeguarding approach and will report any behaviour (of staff, governors, visitors, pupils or parents/carers) which I believe may be inappropriate or concerning in any way to the DSP or Online Safety Leader.

Classroom management of internet access

I will pre-check for appropriateness all internet sites used in the classroom or during a tutoring session; this will include the acceptability of other material visible, however briefly, on the site. I will not free-surf the internet in front of pupils.

If I am using the internet to teach about controversial issues I will secure, on every occasion, approval in advance for the material I plan to use with the schools Headteacher/Head of School.

Video conferencing

I will only use the conferencing tools that have been identified and risk assessed by the school leadership, DDPO and DSP. A school-owned device should be used when running video-conferences, where possible.

User Signature

I agree to follow this Acceptable Use Agreement and to support online safety in my work in the school. I understand this forms part of my company/educational setting/organisation's contract with the school.

Signature

Full Name (printed)

Job Title

Date

Name of school/Trust team	
Requirements for visitors, volunteers and parent/carers helpers (working directly with children or otherwise)	
Online Safety Lead	
Designated Safeguarding Lead (DSP)	

This document is designed to ensure that you are aware of your responsibilities when using any form of IT in the school and other aspects of safeguarding in connection with online safety.

Please raise any safeguarding concerns arising from your visit immediately with the Headteacher and/or DSP.

- I understand I may only use my personal mobile phone(s) and other devices with camera functions in designated areas. When not in a designated area, phones must be switched off and out of sight. Any exception must be pre-arranged;
- I will not take images, sound recording or videos of school events or activities, on or off site, on any device. Any possible exception must be pre-arranged;
- I will not give out my personal details such as mobile phone number, email address, and social media account details to pupils. Where appropriate I may share my professional contact details with parents/carers provided the DSP or Headteacher/Head of School is informed before I leave the school;
- I understand my visit to the school may give me access to privileged information about pupils, staff, school systems and plans. Such information should never be shared on line, including on social media sites;
- I understand I should not use school equipment to access the internet without prior approval from my contact in the school or the Headteacher/Head of School;
- If working in the classroom, I will pre-check for appropriateness all internet sites I intend to use including checking the acceptability of other material visible on the site. I will not free-surf the internet in front of pupils. If I am in any doubt about the appropriateness of the content I plan to use I will check with my contact in the school.

Name of School

Online Safety Acceptable Use Agreement – Key Stage 2 Pupils

Dear Parent/Carer,

The internet, email, mobile technologies and online resources have become an important part of learning and life. We want all children to be safe and responsible when using any IT. It is essential that children are aware of online risk, know how to stay safe and know where to go to report problems or to get help.

Please read through these online safety rules with your child and talk with them to ensure they understand their importance and what it means for them (and for you). When you have done this, you both need to sign this agreement to say that you agree to follow the rules. Any concerns or explanation can be discussed with **Role/Name**.

Please return the signed sections of this form which will be kept on record at the school.

My online safety rules

- I will only use school IT equipment for activities agreed by school staff.
- I will not use my personal email address or other personal accounts in school.
- I will not sign up for any online service on school devices unless this is an agreed part of a school project approved by my teacher and agreed by my parent/carer.
- I will only open email attachments if it has been approved by a member of school staff in school or a parent/carer out of school.
- In school I will only open or delete my files when told by a member of staff.
- I will not tell anyone other than my parents/carers my passwords. I will not use other people's usernames or passwords to pretend to be them online.
- I will make sure that all online contact I make is responsible, polite and sensible. I will be kind and respectful at all times.
- If I come across anything upsetting, unpleasant or nasty, or anything that makes me feel unsafe, I will tell my teacher or my parent/carer immediately.
- If someone says, asks or posts about me anything upsetting, unpleasant or nasty, or anything that makes me feel unsafe, I will not reply. I will tell my teacher, trusted adult or my parent/carer immediately.
- I will not give out my own or other people's personal information, including: name, phone number, home address, interests, schools or clubs. I will tell my teacher or parent/carer if anyone asks me online for personal information.
- Uploading or sending my image (photographs, videos, live streaming) online puts me at risk. I will always seek permission from my teacher or parent/carer if I wish to do this. I will not take, share or upload any image of anyone else without their permission and also, if they are a child, without their parent's/carer's permission.
- Even if I have permission, I will not upload any images, videos, sounds or words that could upset,

now or in the future, any member of the school community, as this is cyberbullying.

- I understand that some people on the internet are not who they say they are and some people are not safe to be in contact with. I will not arrange to meet someone I only know on the internet. If someone asks to meet me, I will not reply to them and I will tell a teacher, trusted adult or a parent/carer immediately.
- I understand that everything I do or receive online can be traced now and in the future. I know it is important to build a good online reputation.
- I understand that some personal devices are allowed in school and some are not, and I will follow the rules. I will not assume that new devices can be brought into school without permission.
- I understand my behaviour in the virtual classroom should mirror that in the physical classroom.
- I will not lie about my age in order to access games, apps or social networks that are for older people as this will put me at risk.
- I understand that these rules are designed to keep me safe now and in the future. If I break the rules my teachers will look into it and may need to take action.

I/we have discussed this agreement, which highlights the associated risks when accessing the internet, mobile and digital technologies, with our child/ren. I/we agree to support them in following the terms of this agreement.

I/we also agree not to share school related information or images online or post material that may bring the school or any individual within it into disrepute.

(Rather than posting negative material online, any parent, distressed or concerned about an aspect of school should make immediate contact with a member of staff. Negative postings about the school would impact on the reputation of the whole school community. Parents are encouraged to report breaches so that we can protect the reputation of the school, staff, pupils and parents).

I/we also agree only to use personal mobile phones and devices in designated areas of the school unless otherwise informed, e.g. for specific events and activities. I/we understand that under no circumstance should images be taken at any time on school premises of anyone other than our own child/ren, unless there is a pre-specified agreement. I/we understand that when on school premises, but not in a designated area where phones can be used, they must be switched off and out of sight.

Pupil agreement

This agreement is to keep me safe. I have discussed this agreement with my parents/carers and understand the commitment I have made and my responsibilities.

Pupil name

Pupil signature

Parent(s)/Carer(s) agreement

Parent(s)/Carer(s) name(s)

Parent/carer signature

Date

Online safety policy guide – Key Information

All Spiral Partnership Trust schools work closely with families to help ensure that children can use internet, mobile and digital technologies safely and responsibly both at home and school. The support of parents/carers is essential to implement the online safety policy effectively and help keep children safe. It is important that parents/carers understand the crucial role they play in this process and the school seeks to regularly consult, discuss and inform in relation to online safety as well as understanding of the benefits of new technologies and associated risks. The school provides regular updated online safety information through the school website, newsletters and by other means.

The school provides online safety information for parents/carers, through the website, in newsletters and at events. It is important that parents/carers understand their key role in supporting children to behave appropriately and keep themselves safe online.

The online safety policy, supported by its acceptable use agreements, is intended to protect the interests and safety of the whole school community.

- All Spiral Partnership Trust schools have online filtering and monitoring systems in place via our broadband provider in line with DfE requirements and strict code of conduct for all staff and others who have access to our online systems.
- Parents/carers are required to support their child in understanding and signing the Online Safety Acceptable Use Agreement for pupils.
- Parents/carers may only use personal mobile phones and devices in designated areas of the school unless otherwise informed, e.g. for specific events and activities. Under no circumstance should images be taken at any time on school premises that include anyone other than their own child, unless there is a pre-specified agreement with individuals and parents/carers. When a parent/carer is on school premises but not in a designated area, their phone/s must be switched off and out of sight.
- Parents/carers should not assume that pupils can bring technological devices to school and should always check with the school. The school is not responsible for the loss, damage or theft of any personal mobile device that is brought into school.
- All cyberbullying incidents affecting children in a Spiral Partnership Trust school should be reported immediately. (If the incident involves an indecent image of a child the report must also be made immediately to the police for your own protection.) The school will investigate and respond to all reported cyberbullying incidents, liaising with others where appropriate. No reply should ever be sent to the sender/poster of cyberbullying content. If applicable block the sender and report abuse to the site. Evidence should be retained and shown in school and/or to the police. Evidence should not be forwarded.
- Online safety is fully embedded within our curriculum. The schools provide a comprehensive age-appropriate curriculum for online safety which enables pupils to become informed, safe and responsible. This includes teaching to prevent radicalisation, for which staff provide a narrative to counter extremism. The PSHE curriculum, Relationships and Health Curriculum are central in supporting the delivery of online safety education.
- The school may choose to set up social media sites, blogs or have some other online presence in its own name. Parents/carers, however, do not have the right to set up any site, page, chat group or any other online presence that uses the Trust or school name or logo in any form.
- Any parent/carer, distressed or concerned about an aspect of school should make immediate contact with a member of staff rather than posting their concerns online. Parents/carers should not share school related information or images online or post material that may bring the school or any individual within it into disrepute. Negative postings about the school would impact on the

reputation of the whole school community. Parents/carers are encouraged to report breaches so that we can protect the reputation of the school, staff, pupils and parents/carers.

Please see the full online safety policy in the policies section on the Trust website.