Policy: ONLINE SAFETY	Status: FINAL	Policy Number: POL_021
Author(s): Vicky Solly	Date of issue: 23 November 2021	Version: V1
Approved by: The Governing Body	Effective: January 2023	Review Date: January 2024

Goodnestone is a place of learning where all are nurtured and supported. Goodnestone has high expectations of all, so they fulfil their God given aspirations within and outside our small school community. Following the example of Jesus, we include all by showing friendship to each other, valuing their unique contribution.

Nonington is a place of learning where all are cared for and supported. Nonington has high expectations of all, so they fulfil their God given aspirations within and outside our small school community. Following the example of Jesus, we trust each other, valuing everyone's unique contribution.

..... * .....

Purpose

Online safety in schools is part of safeguarding at the Federation of Goodnestone & Nonington CE Primary Schools (the Federation). We recognise that the online world evolves so we have policy and procedures in place, which meet statutory guidelines, to keep our pupils, staff and parents safe. We recognise that the online world evolves so we have policy and procedures in place, which meet statutory guidelines, to keep our pupils, staff and parents safe. We have an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones'). We acknowledges its obligation to ensure that all learners and staff are protected from potential online harm.

The Federation believes that the internet and associated devices are an integral part of everyday life. The Federation affirms that all learners should be empowered to build resilience and to develop strategies to recognise and respond to online risks.

Governors and Senior Leadership Team

A governor's role for online safety in a school should include, but is not limited to:

- Upholding online safety as a safeguarding issue which is embedded across the whole school culture.
- Ensuring that children are provided with a safe environment in which to learn and develop.
- Ensuring that the school has appropriate filters and monitoring systems in place and ensuring that an 'appropriate level' of security protection procedures are in place.
-
- Ensuring the school has effective policies and training in place.
- Ensuring that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations.
- Auditing and evaluating online safety practice.
- Ensuring there are robust reporting channels.

Designated Safeguarding Lead (DSL) and Deputy Designated Safeguarding Leads (Deputy DSL)

With respect to online safety, it is the responsibility of the DSL to:

- Ensure children and young people are being appropriately taught about and know how to use the internet responsibly.

Policy: ONLINE SAFETY	Status: FINAL	Policy Number: POL_021
Author(s): Vicky Solly	Date of issue: 23 November 2021	Version: V1
Approved by: The Governing Body	Effective: January 2023	Review Date: January 2024

- Ensure teachers and parents are aware of measures to keep children safe online through relevant training provision.
- Take responsibility for all safeguarding matters, including online safety.
- Manage all online safety issues and incidents in line with the school child protection policy.
- Collaborate with the senior leadership team, the online safety lead and computing lead.
- Facilitate effective record keeping and the reporting and monitoring of all online safety concerns.
- Promote online safety and the adoption of a whole school approach.
- Maintain own training and learning needs, ensuring they are up to date with all matters relating to online safety.

Teachers and Staff

All members of school staff (teaching and non-teaching) have a responsibility to protect children online. This includes every member of staff who works at the school and volunteers. All teachers and staff must always act in accordance with their own professional boundaries, upholding professional behaviour and conduct at all times.

All school staff need to:	Each school will:
• Adhere to all policies in school which support online safety and safeguarding • Maintain compliant procedures when managing data • Model good practice when using technology • Know how to recognise, respond and report signs of online abuse or harm • Use CPOMs to report online concerns	• Ensure provision of robust policies and practices as part of induction and ongoing training provision. • Provide up to date online safety training at least annually or more in line with legislative and statutory changes and/or online safety incidents arising. • Ensure training will include recognition of risks and responding to concerns. • Inform of monitoring and filtering processes. • Make staff aware that their online conduct outside of work can impact upon their professional role and responsibilities. • Advise of appropriate resources. • Ensure that all staff are aware of procedures to follow in recognising, responding and reporting online safety concerns and respond appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline • Ensure that all staff are made aware that: › Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse

Policy: ONLINE SAFETY	Status: FINAL	Policy Number: POL_021
Author(s): Vicky Solly	Date of issue: 23 November 2021	Version: V1
Approved by: The Governing Body	Effective: January 2023	Review Date: January 2024

	◦ Children can abuse their peers online through: ◦ Abusive, harassing, and misogynistic messages ◦ Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups ◦ Sharing of abusive images and pornography, to those who don't want to receive such content ◦ Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element • Ensure that training will also help staff: ◦ develop better awareness to assist in spotting the signs and symptoms of online abuse ◦ develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh them up • develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

Pupils

With respect to online safety in your school, children need to:	Each school will support learner's understanding based on age and ability:	Each school will promote safe and responsible internet use:
• Know who the DSL is. • Engage in age appropriate online safety education opportunities. • Contribute to policy development and review. • Read and adhere to online safety policies. • Respect the feelings of others, both off and online.	• Acceptable use posters in all rooms with internet access. • Informing all learners of monitoring and filtering in place. • Implement peer education strategies. • Provide continuous training and education as part of their transition across key stages.	• Education regarding safe and responsible use and access of the internet. • Include online safety in Personal, Social, Health and Economic (PSHE) education, Relationships and Sex Education (RSE) and Information Computer Technology studies.

Policy: ONLINE SAFETY	Status: FINAL	Policy Number: POL_021
Author(s): Vicky Solly	Date of issue: 23 November 2021	Version: V1
Approved by: The Governing Body	Effective: January 2023	Review Date: January 2024

• Take responsibility for keeping themselves and others safe online. • Where and how to find help with any online incidents or concerns. • How, when and where to report concerns and when to seek help from a trusted adult. • Know what sorts of boundaries are appropriate in friendships with peers and others (including in a digital context), by the end of primary school.	• Use alternative, complementary support where needed. • Seeking learner voice.	• Reinforce online safety messages as a continuum.

Vulnerable children who need our help the most are not only missing out on opportunities to flourish online but are often experiencing the very worst that the online world can be. Over 2 million children in England are living in families with complex needs. Many children are living in families with domestic abuse, parental substance abuse and mental health problems.

The Federation recognises that some learners are more vulnerable due to a range of factors. Those children may be:

- Receiving statutory care or support.
- Known to have experienced specific personal harm.
- With a disability, ill-health or developmental difficulties.
- In households or families with characteristics or locations that indicate higher potential likelihood of current and future harm.
- Vulnerable or of concern by virtue of their identity or nationality.
- At risk in relation to activity or institutions outside the home.
- Caring for others.

Each school will ensure the effective and safe provision of tailored online safety education. Each school will obtain input and advice from specialist staff as deemed necessary.

Parents

Parents need to understand the risks that children face online to protect them from online dangers.

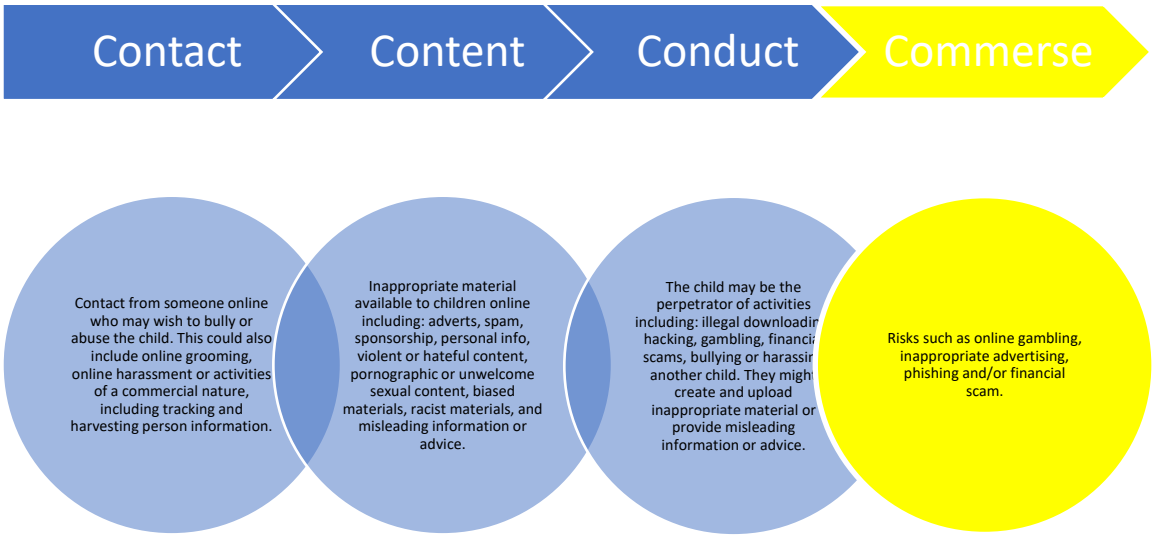
Parents need to:	Each school will:
• Read and adhere to all relevant policies. • Support online safety approaches and education provision.	• Recognise and cultivate the essential role parents and carers have in fostering safer online safety practices in children and young people.

Policy: ONLINE SAFETY	Status: FINAL	Policy Number: POL_021
Author(s): Vicky Solly	Date of issue: 23 November 2021	Version: V1
Approved by: The Governing Body	Effective: January 2023	Review Date: January 2024

• Identify changes in children's behaviour that could indicate they are at risk of online harm or abuse. • Report online issues to the DSL • Be a role model for safe and appropriate behaviour. • Follow the school code of not sharing on social media when taking photos/using technology at school events	• Ensure provision of resources, support and advice. • Ensure provision and adherence to online safety policies and other policies of relevance. • Advise of how and when to raise concerns. • Provide details of all relevant contacts (for example, the DSL).

Types of online risks

Types of online risk usually fall under one of three categories:

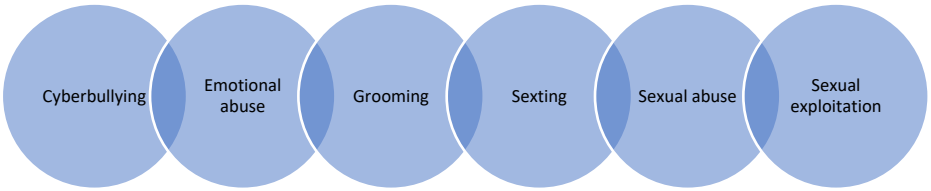


Online Abuse

"Online abuse is any type of abuse that happens on the web, whether through social networks, playing online games or using mobile phones" (NSPCC, 2019).

Hidden harms – types of online abuse may include:

Policy: ONLINE SAFETY	Status: FINAL	Policy Number: POL_021
Author(s): Vicky Solly	Date of issue: 23 November 2021	Version: V1
Approved by: The Governing Body	Effective: January 2023	Review Date: January 2024



The types, patterns and different circumstances of significant harm and abuse should be considered within the categories identified for children: Neglect, Sexual, Physical & Emotional.

Technology can facilitate a world of learning and development in addition to help yield a range of opportunities. However, the stark reality is that it can also present a window to potential and actual harm and abuse. It can elicit and support an array of illegal abusive behaviours including, but not limited to:

This policy should be read alongside the relevant policies relating to safeguarding of children and in addition to the associated statutory legislation and guidance as stipulated on page 1-2 of this policy.

Cultivating a safe environment

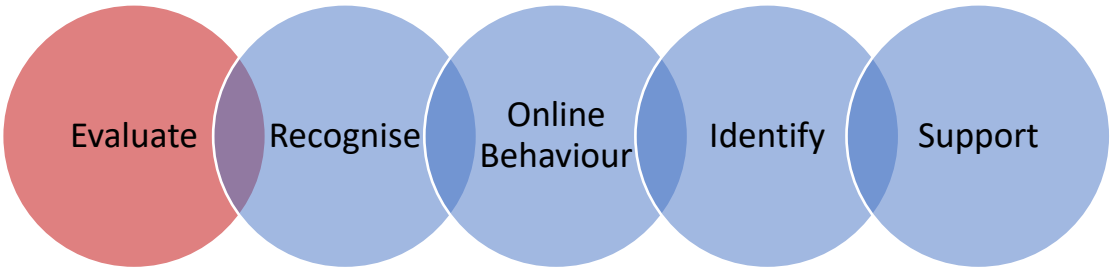
“All staff should be aware of indicators, which may signal that children are at risk from, or are involved with serious violent crime. These may include increased absence from school, a change in friendships or relationships with older individuals or groups, a significant decline in performance, signs of self-harm or a significant change in well-being, or signs of assault or unexplained injuries. Unexplained

Policy: ONLINE SAFETY	Status: FINAL	Policy Number: POL_021
Author(s): Vicky Solly	Date of issue: 23 November 2021	Version: V1
Approved by: The Governing Body	Effective: January 2023	Review Date: January 2024

gifts or new possessions could also indicate that children have been approached by, or are involved with, individuals associated with criminal networks or gangs" (DfE, 2019).

Children should be educated in an age-appropriate way around:

- ✓ **How to evaluate what they see online**
- ✓ **How to recognise techniques for persuasion**
- ✓ **Their online behaviour**
- ✓ **How to identify online risks**
- ✓ **How and when to seek support**

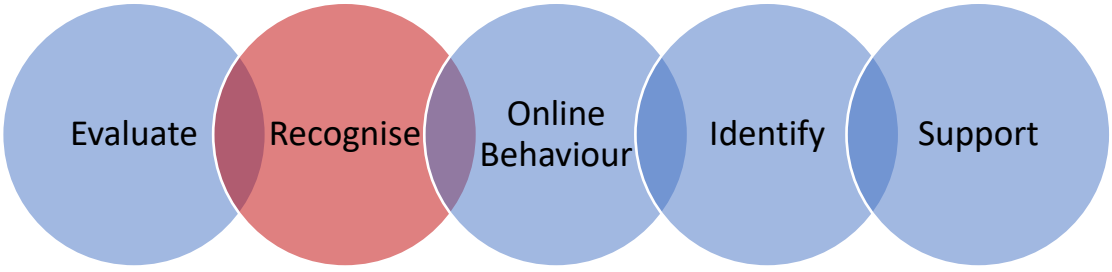


Evaluate: **How to evaluate what they see online**

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

Each school will help pupils to consider questions including:

- Is this website/URL/email fake? How can I tell?
- What does this cookie do and what information am I sharing?
- Is this person who they say they are?
- Why does someone want me to see this?
- Why does someone want me to send this?
- Why would someone want me to believe this?



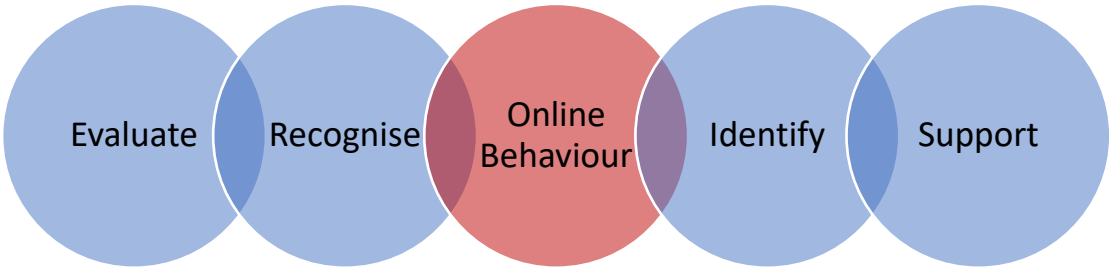
Recognise: How to recognise techniques used for persuasion

Policy: ONLINE SAFETY	Status: FINAL	Policy Number: POL_021
Author(s): Vicky Solly	Date of issue: 23 November 2021	Version: V1
Approved by: The Governing Body	Effective: January 2023	Review Date: January 2024

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

Each school will help pupils to recognise:

- Online content which tries to make people believe something false is true and/or mislead (misinformation and disinformation).
- Techniques that companies use to persuade people to buy something.
- Ways in which games and social media companies try to keep users online longer (persuasive/sticky design)
- Criminal activities such as grooming.



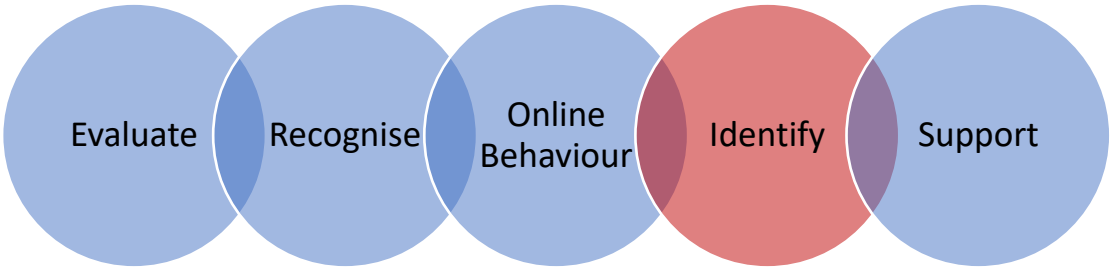
Online Behaviour

This will enable pupils to understand what acceptable and unacceptable online behaviour looks like. Each school will teach pupils that the same standard of behaviour and honesty applies online and offline, including the importance of respect for others. Each school will also teach pupils to recognise unacceptable behaviour in others.

Each school will help pupils to recognise acceptable and unacceptable behaviour by:

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

Policy: ONLINE SAFETY	Status: FINAL	Policy Number: POL_021
Author(s): Vicky Solly	Date of issue: 23 November 2021	Version: V1
Approved by: The Governing Body	Effective: January 2023	Review Date: January 2024



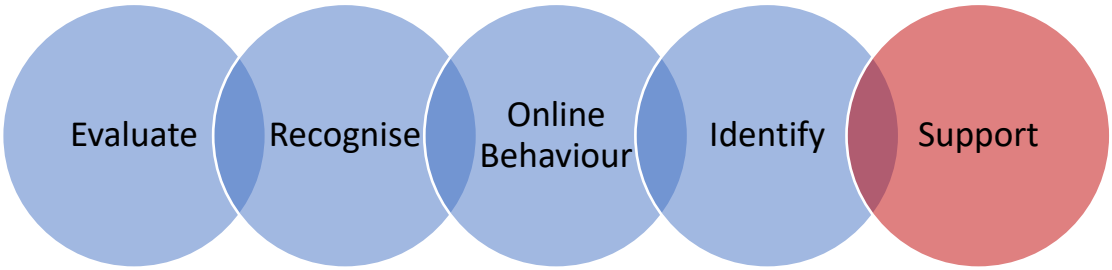
Identify: How to identity online risks

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

Policy: ONLINE SAFETY	Status: FINAL	Policy Number: POL_021
Author(s): Vicky Solly	Date of issue: 23 November 2021	Version: V1
Approved by: The Governing Body	Effective: January 2023	Review Date: January 2024

Each school will help pupils to identify and manage risk by:

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



How and when to seek support

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

Each school will help pupils by:

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

Responding to Online Safety Concerns / incidents

The safety of the child and young person is of paramount importance. Immediate action may be required to safeguard investigations and any other children and young people. Any concern that children and young people may be at risk of harm or abuse must immediately be reported. Reputational issues must be managed appropriately by discussion with the relevant communications team.

Online safety is recognised as part of the education settings safeguarding responsibilities – the DSL should take lead responsibility for online safety concerns which should be recorded and actioned.

Policy: ONLINE SAFETY	Status: FINAL	Policy Number: POL_021
Author(s): Vicky Solly	Date of issue: 23 November 2021	Version: V1
Approved by: The Governing Body	Effective: January 2023	Review Date: January 2024

Children and young people will be enabled (at a level appropriate to their age and ability) to share online concerns. The child protection policy for the federation includes procedures to follow regarding online safety concerns.

Remember:

- Child welfare is of principal concern – the best interests of children take precedence.
- If there is any immediate danger, contact the police on 999.
- Refer to all appropriate agencies as per the federations local process.
- Always adhere to local safeguarding procedures and report to the DSL (Heads of Schools), Executive Headteacher (DDSL):

    - All members of the community will respect confidentiality and the need to follow the official procedures for reporting concerns.
    - Learners, parents and staff will be informed of our complaints procedure and staff will be made aware of the whistleblowing procedure.
    - We require staff, parents, carers and learners to work in partnership with us to resolve online safety issues.
    - After any investigations are completed, leadership staff will debrief, identify lessons learnt and implement any policy or curriculum changes, as required.
    - If we are unsure how to proceed with an incident or concern, the DSL (or deputies) will seek advice from the Education Safeguarding Service.
    - Where there is a concern that illegal activity has taken place, we will contact the police using 101, or 999 if there is immediate danger or risk of harm as appropriate.
    - If information relating to a specific incident or a concern needs to be shared beyond our community, for example if other local settings are involved or the wider public may be at risk, the DSL and Executive Headteacher will speak with the police and/or the Education Safeguarding Service first, to ensure that potential criminal or child protection investigations are not compromised.

Responding to Complaints

There are a number of sources from which a complaint or allegation might arise, including those from:

- A child or young person
- An adult
- A parent/carer
- A member of the public (including a friend or relative)
- A colleague

There may be up to three components in the consideration of an allegation:

- A police investigation of a possible criminal offence.
- Enquiries and assessment by children's social care or adult social care relating to whether a child, young person or adult at risk is in need of protection or services.
- Consideration by an employer of disciplinary action in respect of the individual (including suspension).

It is also the responsibility of the member of staff to inform their line manager if they are being investigated in relation to children, young people or adults at risk with respect to protection concerns

Policy: ONLINE SAFETY	Status: FINAL	Policy Number: POL_021
Author(s): Vicky Solly	Date of issue: 23 November 2021	Version: V1
Approved by: The Governing Body	Effective: January 2023	Review Date: January 2024

outside of work. They should also report if their own children/stepchildren/children they are living with become subject to child protection matters or an adult related to them or living with them become subject to adult protection matters. The line manager must report this to the DSL.

Procedures:

Filtering

- Governors and leaders have ensured that our school has age and ability appropriate filtering and monitoring in place to limit learner's exposure to online risks.
- Our decision regarding filtering and monitoring has been informed by a risk assessment, considering our specific needs and circumstances.
- The school has the ability to block certain words being searched in school.
- Changes to the filtering and monitoring approach will be risk assessed by staff with educational and technical experience, along with school's technical support team and, where appropriate, with consent from the leadership team; all changes to the filtering policy are logged and recorded.
- The leadership team will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate.
- All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard learners; effective classroom management and regular education about safe and responsible use is essential.

Monitoring

- We will appropriately monitor internet use on all setting owned or provided internet enabled devices. This is achieved by:
    - physical monitoring (supervision), monitoring internet and web access (reviewing logfile information) and active technology monitoring services; machines can be monitored in real time and reports can be created for previous dates.
- All users will be informed that use of our systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.
- If a concern is identified via monitoring approaches we will:
    - List how concerns will be responded to e.g. DSL or deputy will respond in line with the child protection policy.

Managing personal data online

- Personal data will be recorded, processed, transferred and made available online in accordance with General Data Protection Regulations and Data Protection legislation.

Security and management of information systems

- We take appropriate steps to ensure the security of our information systems, including:
    - Virus protection being updated regularly.

Policy: ONLINE SAFETY	Status: FINAL	Policy Number: POL_021
Author(s): Vicky Solly	Date of issue: 23 November 2021	Version: V1
Approved by: The Governing Body	Effective: January 2023	Review Date: January 2024

- Encryption for personal data sent over the Internet or taken off site (such as via portable media storage) or access via appropriate secure remote access systems.
- Not downloading unapproved software to work devices or opening unfamiliar email attachments.
- Preventing, as far as possible, access to websites or tools which could compromise our systems, including anonymous browsing and other filtering bypass tools.
- Checking files held on our network, as required and when deemed necessary by leadership staff.
- The appropriate use of user logins and passwords to access our network.
- Specific user logins and passwords will be enforced for all users.
- All users are expected to log off or lock their screens/devices if systems are unattended.

Password policy

- All members of staff have their own unique username and private passwords to access our systems; members of staff are responsible for keeping their password private.
- All learners are provided with their own unique username and private passwords to access our systems; learners are responsible for keeping their password private.
- We require all users to
  - use strong passwords for access into our system.
  - not share passwords or login information with others or leave passwords/login details where others can find them.
  - not to login as another user at any time.
  - lock access to devices/systems when not in use.

Managing the safety of our website

- We will ensure that information posted on our website meets the requirements as identified by the DfE.
- We will ensure that our website complies with guidelines for publications including accessibility, data protection, respect for intellectual property rights, privacy policies and copyright.
- Staff or learner's personal information will not be published on our website; the contact details on the website will be our setting address, email and telephone number.
- The administrator account for our website will be secured with an appropriately strong password.
- We will post appropriate information about safeguarding, including online safety, on our website for members of the community.

Publishing images and videos online

- We will ensure that all images and videos shared online are used in accordance with the associated policies, including (but not limited to) the cameras and image use, data security,

Policy: ONLINE SAFETY	Status: FINAL	Policy Number: POL_021
Author(s): Vicky Solly	Date of issue: 23 November 2021	Version: V1
Approved by: The Governing Body	Effective: January 2023	Review Date: January 2024

acceptable use policies and codes of conduct/behaviour. We require parental permission to share images and videos of pupils in school, on our Facebook page.

Managing email

- Access to our email systems will always take place in accordance with data protection legislation and in line with other policies, including confidentiality, acceptable use of technology policies and the code of conduct policy.
- The forwarding of any chain messages/emails is not permitted.
- Any electronic communication which contains sensitive or personal information will only be sent using secure and encrypted email.
- Setting email addresses and other official contact details will not be used to set up personal social media accounts.
- Members of the community will immediately tell the DSL or deputies if they receive offensive communication, and this will be recorded in our safeguarding records.

Staff email

- All members of staff are provided with an email address to use for all official communication; the use of personal email addresses by staff for any official business is not permitted.
- Members of staff are encouraged to have an appropriate work life balance when responding to email, especially if communication is taking place between staff, learners and parents.

Management of applications (apps) used to record children's progress

- We use Tapestry and Purple Mash to track learners' progress and share appropriate information with parents and carers.
- The school will ensure that the use of tracking systems is appropriately risk assessed prior to use, and that use takes place in accordance with data protection legislation, including the General Data Protection Regulations (GDPR) and Data Protection legislation.
- To safeguard learner's data
    - personal staff mobile phones or devices will not be used to access or upload content to any apps which record and store learners' personal details, attainment or images.
    - devices will be appropriately encrypted if taken off site, to reduce the risk of a data security breach, in the event of loss or theft.
    - all users will be advised regarding safety measures, such as using strong passwords and logging out of systems.
    - parents and carers will be informed of the expectations regarding safe and appropriate use, prior to being given access; for example, not sharing passwords or images.

Social Media

- The expectations' regarding safe and responsible use of social media applies to all members of each schools community.

Policy: ONLINE SAFETY	Status: FINAL	Policy Number: POL_021
Author(s): Vicky Solly	Date of issue: 23 November 2021	Version: V1
Approved by: The Governing Body	Effective: January 2023	Review Date: January 2024

- The term social media may include (but is not limited to) blogs, wikis, social networking sites, forums, bulletin boards, online gaming, apps, video/photo sharing sites, chatrooms and instant messenger.
- All members of each schools community are expected to engage in social media in a positive and responsible manner.
    - All members of each schools community are advised not to post or share content that may be considered threatening, hurtful or defamatory to others on any social media service.
    - The use of social media during each schools hours for personal use is not permitted for staff.
    - The use of social media during each schools hours for personal use is not permitted for learners.
- Concerns regarding the online conduct of any member of each schools community on social media, will be reported to the DSL and be managed in accordance with our anti-bullying, allegations against staff, behaviour and child protection policies.

Staff personal use of social media

- The safe and responsible use of social media sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.
- Safe and professional behaviour will be outlined for all members of staff, including volunteers, as part of our *code of conduct*

Communicating with learners and parents

- Staff will not use personal social media accounts to contact learners or parents/carers, nor should any contact be accepted.
- All members of staff are advised not to communicate with or add any current or past learners or their family members, as 'friends' on any personal social media sites, applications or profiles.
- Any pre-existing relationships or exceptions which compromise this requirement will be discussed with the DSL and the EHT and H of S.
    - Decisions made and advice provided in these situations will be formally recorded in order to safeguard learners, the setting and members of staff.
- Any communication from learners and parents received on personal social media accounts will be reported to the DSL (or deputy) and the EHT and H of S.

Learners use of social media

- Safe and appropriate use of social media will be taught to learners as part of an embedded and progressive education approach via age appropriate sites and resources.
- Any concerns regarding learners use of social media will be dealt with in accordance with existing policies, including anti-bullying and behaviour.
- Concerns regarding learners' use of social media will be shared with parents/carers as appropriate, particularly when concerning underage use of social media services and games.
- Learners will be advised:

Policy: ONLINE SAFETY	Status: FINAL	Policy Number: POL_021
Author(s): Vicky Solly	Date of issue: 23 November 2021	Version: V1
Approved by: The Governing Body	Effective: January 2023	Review Date: January 2024

- to consider the benefits and risks of sharing personal details or information on social media sites which could identify them and/or their location.
- to only approve and invite known friends on social media sites and to deny access to others by making profiles private.
- not to meet any online friends without a parent/carer or other appropriate adults' permission, and to only do so when a trusted adult is present.
- to use safe passwords.
- to use social media sites which are appropriate for their age and abilities.
- how to block and report unwanted communications.
- how to report concerns on social media, both within the setting and externally.

Official use of social media

- The federations official social media channels are: Facebook for both schools; youtube within Nonington
- The official use of social media sites by each school only takes place with clear educational or community engagement objectives and with specific intended outcomes.
- The official use of social media as a communication tool has been formally risk assessed and approved by the Executive Headteacher.
- Executive Headteacher and Heads of School has access to account information and login details for our social media channels.
- Official social media channels have been set up as distinct and dedicated accounts for official educational or engagement purposes only.
    - Executive Headteacher uses setting provided email addresses to register for and manage official social media channels.
    - Official social media sites are suitably protected.
    - Public communications on behalf of the setting will, where appropriate and possible, be read and agreed by at least one other colleague.
- Official social media use will be conducted in line with existing policies, including but not limited to behaviour, image/camera use, data protection, confidentiality and child protection.
- All communication on official social media platforms by staff on behalf of the setting will be clear, transparent and open to scrutiny.
- Any official social media activity involving learners will be moderated.
- Parents and carers will be informed of any official social media use with learners; written parental consent will be obtained, as required.
- We will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.

Mobile Technology: Use of Personal Devices and Mobile Phones

- The federation recognises that personal communication through mobile technologies is part of everyday life for many learners, staff and parents/carers. Mobile technology needs to be used safely and in line with existing policies within the setting.

Policy: ONLINE SAFETY	Status: FINAL	Policy Number: POL_021
Author(s): Vicky Solly	Date of issue: 23 November 2021	Version: V1
Approved by: The Governing Body	Effective: January 2023	Review Date: January 2024

- All use of mobile technology including mobile phones and personal devices such as tablets, games consoles and wearable technology will take place in accordance with our policies, such as behaviour and child protection and with the law.
- Electronic devices of any kind that are brought onto site are the responsibility of the user.
- Mobile phones and personal devices are not permitted to be used in areas that pupils access.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the community; any breaches will be dealt with in line with our anti-bullying and behaviour policies.
- All members of the federation are advised to ensure that their mobile phones and personal devices do not contain any content which may be offensive, derogatory or would otherwise contravene our behaviour or child protection policies.

Staff use of personal devices and mobile phones

- Members of staff will ensure that use of personal phones and devices takes place in accordance with the law, as well as, relevant policy and procedures, such as confidentiality, child protection, data security and acceptable use of technology.
- Staff will be advised to
    - keep mobile phones and personal devices in a safe and secure place during lesson time.
    - keep mobile phones and personal devices switched off or switched to 'silent' mode during lesson times.
    - ensure that Bluetooth or other forms of communication, such as 'airdrop', are hidden or disabled during lesson times.
    - not use personal devices during teaching periods, unless written permission has been given by the Executive Headteacher /Head of School, such as in emergency circumstances.
    - ensure that any content bought onto site via mobile phones and personal devices are compatible with their professional role and expectations.
- Members of staff are not permitted to use their own personal phones or devices for contacting learners or parents and carers.
    - Any pre-existing relationships which could undermine this, will be discussed with the DSL (or deputy) and Executive Headteacher.
- Staff will not use personal devices or mobile phones:
    - to take photos or videos of learners and will only use work-provided equipment for this purpose.
    - directly with learners and will only use work-provided equipment during lessons/educational activities.
- If a member of staff breaches our policy, action will be taken in line with our staff behaviour and allegations policy.
- If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device, or have committed a criminal offence using a personal device or mobile phone, the police will be contacted and the LADO (Local Authority Designated Officer) will be informed in line with our allegations policy.

Policy: ONLINE SAFETY	Status: FINAL	Policy Number: POL_021
Author(s): Vicky Solly	Date of issue: 23 November 2021	Version: V1
Approved by: The Governing Body	Effective: January 2023	Review Date: January 2024

Learners use of personal devices and mobile phones

- Learners will be educated regarding the safe and appropriate use of personal devices and mobile phones and will be made aware of boundaries and consequences.
    - The federation expects learners' personal devices and mobile phones to be handed into the office on arrival at school and phones and devices will be returned to pupils at the end of the school day.
- If a learner needs to contact his/her parents or carers they will be allowed to use the office phone.
    - Parents are advised to contact their child via the school office.
- If a learner breaches the policy, the phone or device will be confiscated and held in the office until the end of the school day, when the learner or parent will collect.
    - Staff may confiscate a learner's mobile phone or device if they believe it is being used to contravene our child protection or behaviour policy.
    - If there is suspicion that material on a learner's personal device or mobile phone may be illegal, or may provide evidence relating to a criminal offence, the device will be handed over to the police for further investigation.
    - Staff may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse includes an online element.

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on screening, searching and confiscation: https://www.gov.uk/government/publications/searching-screening-and-confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people: https://www.gov.uk/government/publications/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people
    -

Visitors' use of personal devices and mobile phones

- Parents/carers and visitors, including volunteers and contractors, are given clear instructions on school's expectations regarding the use of mobile phones and personal devices on site.
- Visitors, including volunteers and contractors, who are on site for regular or extended periods of time are expected to use their mobile phones and personal devices in accordance with our acceptable use of technology policy, child protection and image use.
- Members of staff are expected to challenge visitors if they have concerns and inform the DSL (or deputy) of any breaches of our policy.

Officially provided mobile phones and devices

- The federation mobile phones and devices will be suitably protected via a passcode/password/pin and must only be accessed or used by members of staff.

Policy: ONLINE SAFETY	Status: FINAL	Policy Number: POL_021
Author(s): Vicky Solly	Date of issue: 23 November 2021	Version: V1
Approved by: The Governing Body	Effective: January 2023	Review Date: January 2024

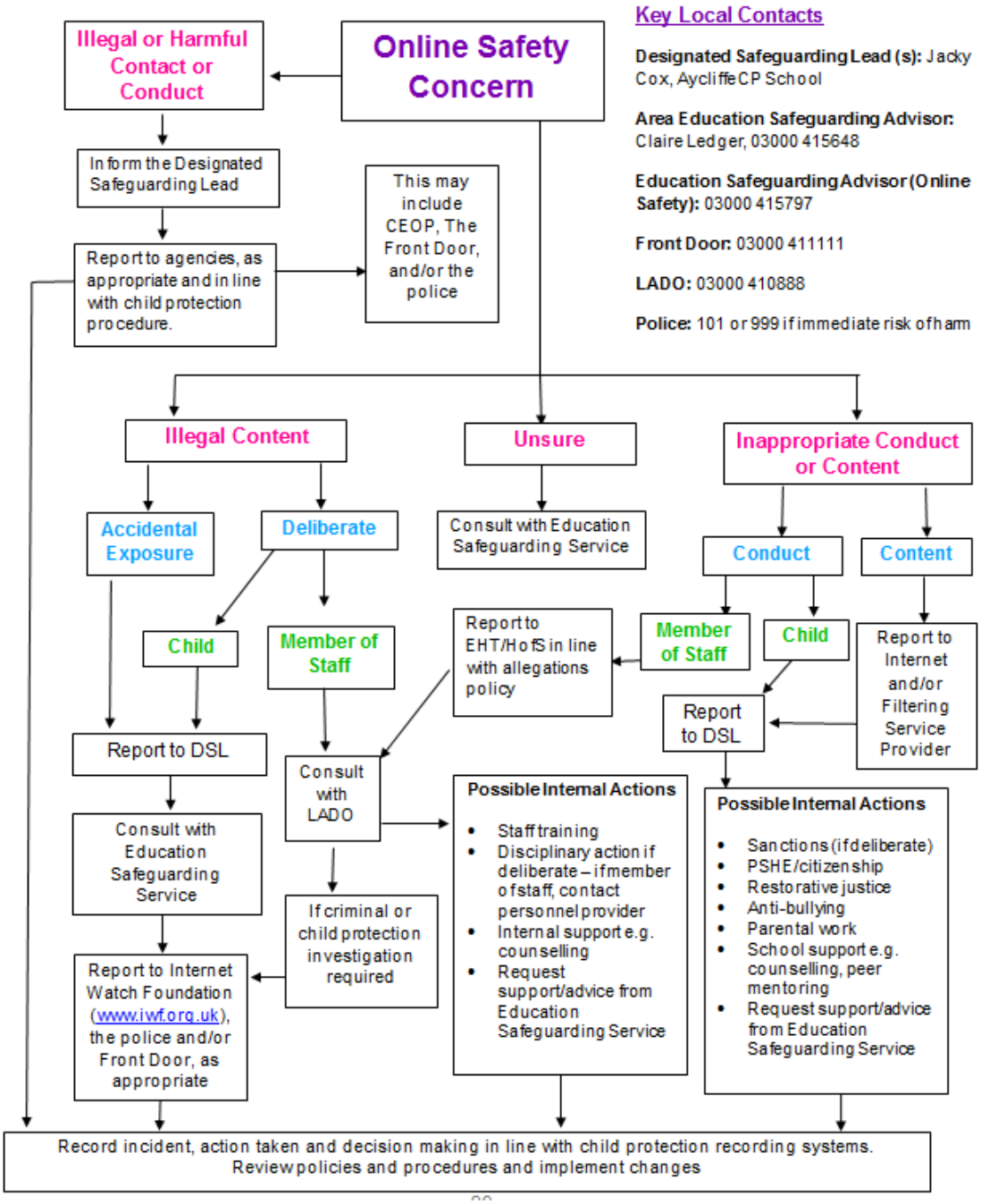
- The federation mobile phones and devices will always be used in accordance with the acceptable use of technology policy and other relevant policies.

Monitoring and Review

- Technology evolves and changes rapidly; as such the federation will review this policy at least annually. At every review, the policy will be shared with the governing board The policy will be revised following any national or local policy updates, any local child protection concerns and/or any changes to our technical infrastructure.
- We will regularly monitor internet use and evaluate online safety mechanisms to ensure that this policy is consistently applied.
- To ensure they have oversight of online safety, the Executive Headteacher / Head of School will be informed of online safety concerns, as appropriate.
- The named governor for safeguarding will report on online safety practice and incidents, including outcomes, on a regular basis to the wider governing body.
- Any issues identified via monitoring policy compliance will be incorporated into our action planning.

Policy: ONLINE SAFETY	Status: FINAL	Policy Number: POL_021
Author(s): Vicky Solly	Date of issue: 23 November 2021	Version: V1
Approved by: The Governing Body	Effective: January 2023	Review Date: January 2024

Responding to an Online Safety Concern Flowchart



Policy: ONLINE SAFETY	Status: FINAL	Policy Number: POL_021
Author(s): Vicky Solly	Date of issue: 23 November 2021	Version: V1
Approved by: The Governing Body	Effective: January 2023	Review Date: January 2024

Appendix 1

Useful Links

Kent Educational Setting Support and Guidance

Education Safeguarding Service, The Education People:

- 03000 415797
  - Rebecca Avery, Education Safeguarding Advisor (Online Protection)
  - Ashley Assiter, Online Safety Development Officer
- Guidance for Educational Settings:
  - www.kelsi.org.uk/support-for-children-and-young-people/child-protection-and-safeguarding
  - www.theeducationpeople.org/blog/?tags=Online+Safety&page=1

KSCMP: www.kscb.org.uk

Kent Police:

- www.kent.police.uk or www.kent.police.uk/internetsafety
- In an emergency (a life is in danger or a crime in progress) dial 999. For non-urgent enquiries, contact Kent Police via 101

Front Door:

- The Front Door can be contacted on 03000 41 11 11
- Out of hours (after 5pm / Urgent calls only) please contact: 03000 41 91 91

Early Help and Preventative Services: www.kelsi.org.uk/special-education-needs/integrated-childrens-services/early-help-contacts

Other:

- EiS – ICT Support for Schools and Kent Schools Broadband Service Desk**:** www.eisit.uk

National Links and Resources for Settings, Learners and Parents/carers

- CEOP:
  - www.thinkuknow.co.uk
  - www.ceop.police.uk
- Internet Watch Foundation (IWF): www.iwf.org.uk
- UK Council for Internet Safety (UKCIS): www.gov.uk/government/organisations/uk-council-for-internet-safety
- UK Safer Internet Centre: www.saferinternet.org.uk
  - Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline
  - Report Harmful Content: https://reportharmfulcontent.com/

Policy: ONLINE SAFETY	Status: FINAL	Policy Number: POL_021
Author(s): Vicky Solly	Date of issue: 23 November 2021	Version: V1
Approved by: The Governing Body	Effective: January 2023	Review Date: January 2024

- 360 Safe Self-Review tool for schools: www.360safe.org.uk
- Childnet: www.childnet.com
  - Step Up Speak Up – Online Sexual Harassment Guidance: www.childnet.com/resources/step-up-speak-up/guidance-and-training-for-schools-and-professionals
  - Cyberbullying Guidance: www.childnet.com/resources/cyberbullying-guidance-for-schools
- Internet Matters: www.internetmatters.org
- Parent Zone: https://parentzone.org.uk
- Parent Info: https://parentinfo.org
- NSPCC: www.nspcc.org.uk/onlinesafety
  - ChildLine: www.childline.org.uk
  - Net Aware: www.net-aware.org.uk
- Lucy Faithfull Foundation: www.lucyfaithfull.org
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- Action Fraud: www.actionfraud.police.uk
- Get Safe Online: www.getsafeonline.org

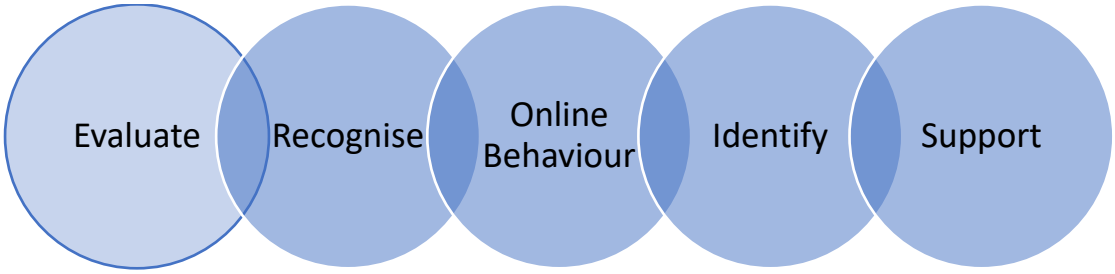
Policy: ONLINE SAFETY	Status: FINAL	Policy Number: POL_021
Author(s): Vicky Solly	Date of issue: 23 November 2021	Version: V1
Approved by: The Governing Body	Effective: January 2023	Review Date: January 2024

Appendix 2

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS

I will read and follow the rules in the acceptable use agreement policy

When I use the school's ICT systems (like computers) and use the internet in school I will:



- **Evaluate** - study carefully what I see online so that I do not assume that it is true or acceptable
- **Recognise** – with the help of my teachers, recognise the techniques that are often used to persuade or manipulate others
- **Online Behaviour** – with the help of my teachers, recognise and understand what acceptable and unacceptable behaviour looks like, including the importance of respect for others
- **Identify** - with the help of my teachers, recognise online risks and make sensible and safe decisions about how to act
- **Support** - with the help of my teachers, understand and know safe ways in which to get support if I am concerned or upset by something I have seen online.
- will always use the school's ICT systems and the internet responsibly and for educational purposes only
- will only use them when a teacher is present
- will only use my login and password and not share these with others
- will keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent (school and home)
- will turn my screen off immediately and tell a teacher (or trusted adult) immediately if I find any material which might upset, distress or harm me or others
- always log off or shut down a computer when I'm finished working on it
- will only open and delete my own files (school and home)
- understand that the school can check my computer use and that my parents/carers can be contacted if school staff are concerned about my safety

Policy: ONLINE SAFETY	Status: FINAL	Policy Number: POL_021
Author(s): Vicky Solly	Date of issue: 23 November 2021	Version: V1
Approved by: The Governing Body	Effective: January 2023	Review Date: January 2024

- will not deliberately look for, save or send anything that could be unpleasant or nasty (school and home)

If I bring a personal mobile phone or other personal electronic device into school:

- I will hand it to my teacher for safe keeping and collect it at the end of the day.
- I will use my phone responsibly outside of school, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online

Signed (pupil):	**Date:**
Parent agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these. I will support online safety approaches and education provision.	
Signed (parent/carer):	**Date:**

Policy: ONLINE SAFETY	Status: FINAL	Policy Number: POL_021
Author(s): Vicky Solly	Date of issue: 23 November 2021	Version: V1
Approved by: The Governing Body	Effective: January 2023	Review Date: January 2024

Appendix 3

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS,VOLUNTEERS AND VISITORS	
Name of staff member/governor/volunteer/visitor:	
When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) • Use them in any way which could harm the school's reputation • Access social networking sites or chat rooms • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software, or connect unauthorised hardware or devices to the school's network • Share my password with others or log in to the school's network using someone else's details • Take photographs of pupils without checking with teachers first • Share confidential information about the school, its pupils or staff, or other members of the community • Access, modify or share data I'm not authorised to access, modify or share • Promote private businesses, unless that business is directly related to the school	
I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	**Date:**

Policy: ONLINE SAFETY	Status: FINAL	Policy Number: POL_021
Author(s): Vicky Solly	Date of issue: 23 November 2021	Version: V1
Approved by: The Governing Body	Effective: January 2023	Review Date: January 2024

Appendix 4

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	**Date**:
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are you aware of the ways pupils can abuse their peers online?	
Are there any areas of online safety in which you would like training/further training?	

Policy: ONLINE SAFETY	Status: FINAL	Policy Number: POL_021
Author(s): Vicky Solly	Date of issue: 23 November 2021	Version: V1
Approved by: The Governing Body	Effective: January 2023	Review Date: January 2024

..... * .....

The Federation of Goodnestone and Nonington CE Schools recognise that all pupils are equal regardless of cultural or ethnic background, religion, social circumstances, gender, sexual orientation, ability and disability. The curriculum and whole ethos of the school demonstrates that diversity is understood, is welcomed and appreciated within the school. Equal opportunities means that all children have the right to a broad and balanced curriculum with which all pupils can engage and achieve.