On Line Safety Policy				
Date	Review Date	Lead DSL and Deputy DSL	IT Manager	Nominated Governor
October 2026	October 2027	Jane Maclennan Sharon Moy	Michael Gedge	Daniel Childerhouse (Chair of Governors)

Designated Safeguarding Lead(s):

- Jane Maclennan, Deputy Headteacher and Designated Safeguarding Lead
- Sharon Moy, Deputy Designated Safeguarding Lead
- Debbie Edwards Headteacher
- Jess Saddler SENDCO

Future Education Online Safety Policy

Policy Aims

- This online safety policy has been written by Future Education, involving staff, learners and parents/carers.
- It takes into account the DfE statutory guidance Keeping children safe in education - GOV.UK (www.gov.uk) 2026 'Working Together to Safeguard Children' 2026 and the Norfolk Safeguarding Children Board, www.norfolklscb.org procedures.
- The purpose of Future Education's online safety policy is to:
- Have robust processes in place to ensure online safety of pupils. Staff. Volunteers and governors.
- Identify and support groups of pupils that are potentially at greater risk of harm online than others.
- Deliver 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
- Future Education identifies that the issues classified within online safety are considerable, but can be broadly categorised into four key areas of risk:
- **Content**: being exposed to illegal, inappropriate or harmful material
- **Contact**: being subjected to harmful online interaction with other users
- **Conduct**: personal online behaviour that increases the likelihood of, or causes, harm.
- **Commerce**: risks such as online gambling. Inappropriate advertising, phishing and or financial scams

Policy Scope

Future Education believes that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all learners and staff are protected from potential harm online.

Future Education identifies that the internet and associated devices, such as computers, tablets, mobile phones and games consoles, are an important part of everyday life.

Future Education believes that learners should be empowered to build resilience and to develop strategies to manage and respond to risk online.

This policy applies to all staff including the governing body, leadership team, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the setting (collectively referred to as "staff" in this policy) as well as learners, parents and carers.

This policy applies to all access to the internet and use of technology, including personal devices, or where learners, staff or other individuals have been provided with setting issued devices for use off-site, such as a work laptops, tablets or mobile phones.

Links with other policies and practices

This policy links with several other policies, practices and action plans including:

- Anti-bullying policy
- School Personnel Code of Conduct
- Relationships and Behaviour policy
- Whole School Safeguarding Policy
- Data Protection (GDPR) Policy

Monitoring and Review

- Technology in this area evolves and changes rapidly. Future Education will review this policy at least annually.
- The policy will also be revised following any national or local policy requirements, any child protection concerns or any changes to the 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, Head Teacher and lead DSL will be informed of online safety concerns.
- Any issues identified via monitoring will be incorporated into our action planning.

Roles and Responsibilities

- The Designated Safeguarding Lead (DSL) Jane Maclennan has lead responsibility for online safety. Whilst activities of the designated safeguarding lead may be delegated to an appropriately trained deputy(Sharon Moy) overall the ultimate lead responsibility for safeguarding and child protection, including online safety remains with the Lead DSL.
- Future Education recognises that all members of the community have important roles and responsibilities to play with regards to online safety.

The Leadership and Management Team will:

- Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.
- Ensure there are appropriate and up-to-date policies regarding online safety; including a staff code of conduct and relationships and behaviour policy
- Ensure that suitable and appropriate filtering and monitoring systems are in place and work with technical staff to monitor the safety and security of our systems and networks.
- Ensure that online safety is embedded within a progressive curriculum, which enables all learners to develop an age-appropriate understanding of online safety.
- Support the DSL and any deputies by ensuring they have sufficient time and resources to fulfil their online safety responsibilities.
- Ensure there are robust reporting channels for the community to access regarding online safety concerns, including internal, local and national support.
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology.
- Audit and evaluate online safety practice to identify strengths and areas for improvement.

The Designated Safeguarding Lead (DSL) will:

- Act as a named point of contact on all online safeguarding issues and liaise with other members of staff or other agencies, as appropriate.

- Work alongside deputy DSLs to ensure online safety is recognised as part of the settings safeguarding responsibilities and that a coordinated approach is implemented.
- Ensure all members of staff receive regular, up-to-date and appropriate online safety training.
- Access regular and appropriate training and support to ensure they understand the unique risks associated with online safety and have the relevant up to date knowledge to keep learners safe online.
- Access regular and appropriate training and support to ensure they recognise the additional risks that learners with SEN and disabilities (SEND) face online.
- Keep up-to-date with current research, legislation and trends regarding online safety and communicate this with the community, as appropriate.
- Ensure that online safety is promoted to parents, carers and the wider community, through a variety of channels and approaches.
- Maintain records of online safety concerns, as well as actions taken, as part of the settings safeguarding recording mechanisms.
- Monitor online safety incidents to identify gaps and trends, and use this data to update the education response, policies and procedures.
- Report online safety concerns, as appropriate, to the Leadership team and Governing Body.
- Work with the leadership team to review and update online safety policies on a regular basis (at least annually) with stakeholder input.
- Meet regularly with the safeguarding governor

It is the Responsibility of all Members of Staff to:

- Contribute to the development of online safety policies.
- Read and adhere to the online safety policy.
- Know the DSL responsible for filtering and monitoring.
- Report all online safety concerns via **CPOMS in line with whole school safeguarding policy.**
- Take responsibility for the security of setting systems and the data they use or have access to.
- Model good practice when using technology and maintain a professional level of conduct in their personal use of technology, both on and off site.
- Embed online safety education in curriculum delivery, wherever possible.
- Have an awareness of a range of online safety issues and how they may be experienced by the children in their care.
- Identify online safety concerns and take appropriate action by following the settings safeguarding policies and procedures.
- Know when and how to escalate online safety issues, including signposting to appropriate support, internally and externally.
- Take personal responsibility for professional development in this area.

It is the Responsibility of the IT Manager to:

- Provide technical support and perspective to the DSL and leadership team, especially in the development and implementation of appropriate online safety policies and procedures.
- Oversee the running of Smoothwall (Filtering and monitoring system)
- Implement appropriate security measures as directed by the DSL and leadership team (such as password policies and encryption) to ensure that the settings IT infrastructure/system is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.
- Ensure that our filtering policy is applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team.
- Ensure that filtering and monitoring requirements ensure that the use of generative AI is used safely

- Ensure that our monitoring systems are applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team
- Ensure appropriate access and technical support is given to the DSL (and/or deputy) to our filtering and monitoring systems, to enable them to take appropriate safeguarding action if/when required.
- Maintain an awareness of technical developments which may affect the school's online policies and procedures, and work with the leadership team to make adjustments as required
-

At Future Education we would ask that pupils

Engage in age appropriate online safety education opportunities.

- Contribute to the development of online safety policies.
- Respect the feelings and rights of others both on and offline.
- Take responsibility for keeping themselves and others safe online.
- Seek help from a trusted adult, if there is a concern online, and support others that may be experiencing online safety issues.

At Future Education we would ask that parents and carers

- Support our online safety approaches by discussing online safety issues with their children and reinforcing appropriate and safe online behaviours at home.
- Role model safe and appropriate use of technology and social media.
- Identify changes in behaviour that could indicate that their child is at risk of harm online.
- Seek help and support from the setting, or other appropriate agencies, if they or their child encounter risk or concerns online.
- Contribute to the development of the online safety policies.
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies
- Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites:
- What are the issues? – UK Safer Internet Centre
- Help and advice for parents/carers – Childnet
- Parents and carers resource sheet – Childnet

Educating pupils about online safety

In KS3 and 4 , pupils will be taught to:

To understand how changes in technology affect safety, including new ways to protect their online privacy and identity

How to report a range of concerns

By the end of their time at Future Education, pupils understand

Rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online

Online risks, including the importance of being cautious about sharing personal information online and of using privacy and location settings appropriately to protect information online. Pupils should also understand the difference between public and private online spaces and related safety issues

The characteristics of social media, including that some social media accounts are fake, and/or may post things which aren't real/have been created with AI. That social media users may say things in more extreme ways than they might in face-to-face situations, and that some users present highly exaggerated or idealised profiles of themselves online

Not to provide material to others that they would not want to be distributed further and not to pass on personal material which is sent to them. Pupils should understand that any material provided online might be circulated, and that once this has happened there is no way of controlling where it ends up. Pupils should understand the serious risks of sending material to others, including the law concerning the sharing of images

That keeping or forwarding indecent or sexual images of someone under 18 is a crime, even if the photo is of themselves or of someone who has consented, and even if the image was created by the child and/or using AI-generated imagery. Pupils should understand the potentially serious consequences of acquiring or generating indecent or sexual images of someone under 18, including the potential for criminal charges and severe penalties including imprisonment. Pupils should know how to seek support and should understand that they will not be in trouble for asking for help, either at school or with the police, if an image of themselves has been shared. Pupils should also understand that sharing indecent images of people over 18 without consent is a crime

What to do and how to report when they are concerned about material that has been circulated, including personal information, images or videos, and how to manage issues online

About the prevalence of deepfakes including videos and photos, how deepfakes can be used maliciously as well as for entertainment, the harms that can be caused by deepfakes and how to identify them

That the internet contains inappropriate and upsetting content, some of which is illegal, including unacceptable content that encourages misogyny, violence or use of weapons. Pupils should be taught where to go for advice and support about something they have seen online. Pupils should understand that online content can present a distorted picture of the world and normalise or glamorise behaviours which are unhealthy and wrong

That social media can lead to escalations in conflicts, how to avoid these escalations and where to go for help and advice

How to identify when technology and social media is used as part of bullying, harassment, stalking, coercive and controlling behaviour, and other forms of abusive and/or illegal behaviour and how to seek support about concerns

That pornography, and other online content, often presents a distorted picture of people and their sexual behaviours and can negatively affect how people behave towards sexual partners. This can affect pupils who see pornographic content accidentally as well as those who see it deliberately. Pornography can also portray misogynistic behaviours and attitudes which can negatively influence those who see it

How information and data is generated, collected, shared and used online

That websites may share personal data about their users, and information collected on their internet use, for commercial purposes (e.g. to enable targeted advertising)

That criminals can operate online scams, for example using fake websites or emails to extort money or valuable personal information. This information can be used to the detriment of the person or wider society. About risks of sextortion, how to identify online scams relating to sex, and how to seek support if they have been scammed or involved in sextortion

That AI chatbots are an example of how AI is rapidly developing, and that these can pose risks by creating fake intimacy or offering harmful advice. It is important to be able to critically think about new types of technology as they appear online and how they might pose a risk

The safe use of social media and the internet will also be covered in other subjects where relevant.
Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

Pupils will be taught practical cyber security skills

The following items come from the DfE's non-statutory cyber security standards for schools and colleges.

All pupils will receive age-appropriate training on safe internet use, including:

Methods that hackers use to trick people into disclosing personal information

Password security

Social engineering

The physical security of devices

The risks of removable storage devices (e.g. USBs)

Multi-factor authentication

How to report a cyber incident or attack

How to report a personal data breach

- Future Education will establish and embed a progressive online safety curriculum to raise awareness and promote safe and responsible internet use amongst learners by:
- Ensuring education regarding safe and responsible use precedes internet access.
- Including online safety in Personal, Social, Health and Economic (PSHE), Relationships and Sex Education (RSE) and computing programmes of study.
- Reinforcing online safety messages whenever technology or the internet is in use.
- Educating learners in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation. Teaching learners to be critically aware of the materials they read and show how to validate information before accepting its accuracy.
- Future Education will support learners to understand the acceptable use in a way which suits their age and ability by:
- Displaying acceptable use posters in all rooms with internet access.
- Informing learners that network and internet use will be monitored for safety and security purposes and in accordance with legislation.
- Rewarding positive use of technology.
- Implementing appropriate peer education approaches.
- Seeking learner voice when writing and developing online safety policies and practices, including curriculum development and implementation.
- Using support, such as external visitors, where appropriate, to complement and support our internal online safety education approaches.

Vulnerable learners

- Future Education recognises that, as school for students with SEMH, learners are more vulnerable online due to a range of factors. This may include, but is not limited to children in care, children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss.
- Future Education will ensure that differentiated online safety education, access and support is provided to vulnerable learners.
- When implementing an appropriate online safety policy and curriculum Future Education will seek input from specialist staff as appropriate, including the SENDCO, Looked After Children Designated Teacher, IT Manager etc.

Artificial intelligence (AI)

Generative AI tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Gemini.

Future Education recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes' or 'deep nudes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

Future Education will treat any use of AI to bully pupils very seriously, in line with our Behaviour and Relationships and Safeguarding policy.

Training and engagement with staff.

We will:

- Provide and discuss the online safety policy and procedures with all members of staff as part of induction.
- Provide up-to-date and appropriate online safety training for all staff on a regular basis, with regular updates.
- This will be included in ongoing and regular safeguarding training and through specific online and e-safety training.
- This will cover the potential risks posed to learners (Content, Contact and Conduct) as well as our professional practice expectations.
- Make staff aware that our IT systems are monitored, and that activity can be traced to individual users; staff will be reminded to behave professionally and in accordance with our policies when accessing our systems and devices.
- Make staff aware that their online conduct outside of the setting, including personal use of social media, could have an impact on their professional role and reputation (see school personnel code of conduct).
- Highlight useful educational resources and tools which staff should use, according to the age and ability of the learners.
- Ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting learners, colleagues or other members of the community.

Awareness and engagement with parents and carers

- Future Education recognises that parents and carers have an essential role to play in enabling children and young people to become safe and responsible users of the internet and associated technologies.
- We will build a partnership approach to online safety with parents and carers by: Providing information and guidance on online safety in a variety of formats.
- Drawing their attention to the online safety policy and expectations in newsletters, letters, and on our website.
- Requesting that they read online safety information as part of joining our community, for example, within our home school agreement.

Reducing online risks

Future Education recognises that the internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace.

We will:

- Regularly review the methods used to identify, assess and minimise online risks.
- Examine emerging technologies for educational benefit and undertake appropriate risk assessments before use in the setting is permitted.

- Ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material.

Due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via our computers or devices.

All members of the community are made aware of our expectations regarding safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos which could cause harm, distress or offence to members of the community. This is clearly outlined in our code of conduct.

Safer Use of Technology

Classroom use.

Future Education uses a wide range of technology. This includes access to; computers, laptops and other digital devices

All setting owned devices will be used in accordance with our acceptable use policies and with appropriate safety and security measures in place.

Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.

We will ensure that the use of internet-derived materials, by staff and learners complies with copyright law and acknowledge the source of information.

Learners will be appropriately supervised when using technology, according to their ability and understanding.

Filtering and monitoring

- Future Education will monitor and filter access to the intent through the school's systems as appropriate as per the DFE guidance' – Meeting digital and technology standards in schools and colleges – Cyber security standards for schools – Guidance – GOV.UK (www.gov.uk).

Future Education uses Smoothwall

Smoothwall works by combining real-time web filtering and active digital monitoring to protect students from harmful online content and flag potential safeguarding risks.
It operates through two main products—Smoothwall Filter and Smoothwall Monitor—which function differently to manage web access and user behaviour.

Smoothwall Filter (Web Access Prevention)

Real-time content analysis: Instead of relying only on static blocklists of URLs, the Smoothwall Web Filter scans the copy, content, and context of every web page at the exact moment it is requested.

Granular logic: It uses "Who, What, Where, and When" rules to customise internet access for different groups of users at different times of the day.

Smoothwall Monitor

Background tracking: The Smoothwall Monitor software runs in the background capturing text typed and screenshots taken by users.

Offline functionality: It records activity even when the device is offline, uploading the stored data to the cloud as soon as an internet connection is restored.

- AI and human moderation: Artificial intelligence grades the risk of captured text or images. Potential risks are reviewed by trained human moderators to filter out false alarms.
- Alert notifications: If a risk is verified, Designated Safeguarding Leads (DSLs) at the school receive instant alerts via email or phone calls for critical incidents, allowing for fast intervention.
- Once the alert has been sent The DSL will follow procedure in line with whole school safeguarding policy. Incident will be recorded on CPOMS and where necessary parents and other agencies will be alerted.

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.

Filtering

We use Smoothwall filtering to stop internet users from accessing unapproved websites. We block sites which can be categorised as: pornography, racial hatred, extremism, gaming and sites of an illegal nature. Any unclassified websites are blocked as a precaution.

All devices on-site as well as Future Education owned devices off-site are filtered.

Smoothwall running on our servers identifies a user trying to access webpages allowing Future Education to specify different restrictions for different users, and also allows us to monitor user activity.

If learners discover unsuitable sites:

- The student will be asked to switch off the monitor/screen and notify the classroom teacher (or other member of staff) immediately
- The member of staff will report the concern to the DSL (or deputy)
- The breach will be recorded and escalated as appropriate.
- Parents/carers will be informed of filtering breaches involving their child.

Staff and guests using BYOD (Personal mobile phones) use DNS Filtering at the Smoothwall device to block harmful sites transparently. BYOD devices do not authenticate and so users of these devices may not be known but are subject to student level filtering. Students are prohibited from connecting BYOD to our network.

Monitoring

Through Smoothwall We will appropriately monitor internet use on all Future Education owned or provided internet enabled devices.

This is achieved by:

- Smoothwall identifies users trying to access webpages.
- Smoothwall identifies searches that students are making on school computers
- If a user is blocked from accessing a website a notification email is sent to DSLs
- Smoothwall will notify DSL's of any breaches of filtering
- Smoothwall adds a 'grade of risk' to the concern.
- DSL's receive regular alerts.
- Classroom management is still the primary means of monitoring access and staff take responsibility for overseeing pupils' use of the internet in their respective classes
- If a concern is identified via monitoring approaches, the DSL will respond in accordance with the Whole School Safeguarding Policy.
- 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.

Managing personal data online

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

Security management of online systems

We take appropriate steps to ensure the security of our information systems, including:

- Virus protection being updated regularly.
- 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 using portable media without specific permission; portable media will be checked by an anti-virus /malware scan before use.
- Not downloading unapproved software to work devices or opening unfamiliar email attachments.
- Regularly checking files held on our network, the appropriate use of user logins and passwords to access our network.
- All users are expected to log off or lock their screens/devices if systems are unattended.

Password policy

All members of staff will 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.

Learners' passwords are not changed regularly as their SEND needs affect their ability to do this. Access to user accounts is however monitored and managed We require staff users to:

- Use strong passwords for access into our system.
- Change their passwords every 60 days
- Always keep their password private; users must not share it with others or leave it where others can find it.
- Not to login as another user at any time.

Managing the safety of our website.

We will ensure that information posted on our website meets the requirements as identified by the Department for Education (DfE) for independent special schools.

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

We will ensure that all images and videos shared online are used in accordance with the associated polices, including (but not limited to) the: cameras and image use, data security, acceptable use policies, codes of conduct/behaviour, social media and use of personal devices and mobile phones.

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 policies and the code of conduct/behaviour policy.
The forwarding of any chain messages/emails is not permitted.
Spam or junk mail will be blocked and reported to the email provider.
Any electronic communication which contains sensitive or personal information will only be sent using secure and encrypted email in accordance with the GDPR Policy
Setting email addresses and other official contact details will not be used for setting up personal social media accounts.
Members of the community will immediately tell The Head Teacher if they receive offensive communication, and this will be recorded in our safeguarding files/records.
Excessive social email use can interfere with teaching and learning and will be restricted; access to external personal email accounts may be blocked on site.

Staff Email

The use of personal email addresses by staff for any official setting business is not permitted.
All members of staff are provided with an email address to use for all official communication.
Members of staff are encouraged to have an appropriate work life balance when responding to email.

Learner Email

Learners are issued with their own email addresses in order that they can receive emails securely.
Learners inbound and outbound email is moderated by the Head Teacher and DSL Lead and must be approved before the email is sent or received.

Social media.

Expectations

The expectations' regarding safe and responsible use of social media applies to all members of Future Education community.
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 Future Education community are expected to engage in social media in a positive, safe and responsible manner.
- All members of Future Education community are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.
- We will control learner and staff access to social media whilst using setting provided devices and systems on site.

Concerns regarding the online conduct of any member of Future Education community on social media, should be reported to the Head teacher and will be managed in accordance with our anti-bullying, allegations against staff, school personnel code of conduct, behaviour and child protection policies.

Staff personal use of social media

The safe and responsible use of social networking, social media and personal publishing 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 School Personnel Code of Conduct (see linked policy)

Reputation

All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within the setting.

Civil, legal or disciplinary action may be taken if staff are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

All members of staff are advised to safeguard themselves and their privacy when using social media sites. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis. This will include (but is not limited to):

- Setting the privacy levels of their personal sites.
- Being aware of location sharing services.
- Opting out of public listings on social networking sites.
- Logging out of accounts after use.
- Keeping passwords safe and confidential.
- Ensuring staff do not represent their personal views as that of the setting.
- Members of staff are encouraged not to identify themselves as employees of Future Education on their personal social networking accounts; this is to prevent information on these sites from being linked with the setting, and to safeguard the privacy of staff members.
- All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance our policies and the wider professional and legal framework.
- Information and content that staff members have access to as part of their employment, including photos and personal information about learners and their family members or colleagues will not be shared or discussed on social media sites.
- Members of staff will notify the Leadership Team immediately if they consider that any content shared on social media sites conflicts with their role.

Communicating with learners and parents and carers

All members of staff are advised not to communicate with or add as ‘friends’ any current or past learners or their family members via any personal social media sites, applications or profiles. More information is included in the school personnel code of conduct policy.

Staff will not use personal social media accounts to contact learners or parents, nor should any contact be accepted, except in circumstance whereby prior approval has been given by the Head Teacher

Any communication from learners and parents received on personal social media accounts will be reported to the DSL (or deputy).

Learners use of social media

Safe and appropriate use of social media will be taught to learners as part of an embedded and progressive educational 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 relationships and behaviour policy.

Concerns will be shared with parents/carers as appropriate, particularly when concerning underage use of social media sites, games or tools.

Learners will be advised: - To consider the benefits and risks of sharing personal details 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 responsible adult's permission and only 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 both within the setting and externally.

Student Use of Personal Devices and Mobile Phones

In line with statutory guidance, our school is a mobile phone-free environment by default. Pupils are not permitted to have access to or use their mobile phones or smart technology with similar functionality to mobile phones (e.g. smart watches), which we refer to collectively as 'mobile phones', throughout the school day. This prohibition includes all lessons, the time between lessons, breaktimes, and lunchtimes.

Any deviation from this mobile phone-free baseline will be by exception only (for example, approved arrangements for specific medical tracking or documented safeguarding needs) and must be explicitly authorised by the headteacher.

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.

Staff will be advised to:

- Staff should not use their mobile phone or personal device at any time during the school day unless it is in the staffroom or private office.
- Keep mobile phones and personal devices in a safe and secure place throughout the school day
- Not use personal devices during teaching periods, unless explicit permission has been given by the Head Teacher 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/or Head Teacher
- Staff will not use personal devices: To take photos or videos of learners and will only use work provided equipment for this purpose. Staff 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 code of conduct/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, the police will be contacted.

Learners use of personal devices and mobile phones

In line with statutory guidance, our school is a mobile phone-free environment by default. Pupils are not permitted to have access to or use their mobile phones or smart technology with similar functionality to mobile phones (e.g. smart watches), which we refer to collectively as 'mobile phones', throughout the school day. This prohibition includes all lessons, the time between lessons, breaktimes, and lunchtimes.

Any deviation from this mobile phone-free baseline will be by exception only (for example, approved arrangements for specific medical tracking or documented safeguarding needs) and must be explicitly authorised by the headteacher.

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.
If a learner needs to contact his/her parents or carers they will be allowed to use an office phone. Parents are advised to contact their child via the school office

Mobile phones and personal devices must not be taken into examinations.

Learners found in possession of a mobile phone or personal device during an exam will be reported to the appropriate examining body. This may result in the withdrawal from either that examination or all examinations.

If a learner breaches the policy, the phone or device will be confiscated and will be held in a secure place.

Staff may confiscate a learner's mobile phone or device if they believe it is being used to contravene our behaviour or bullying policy or could contain youth produced sexual imagery (sexting).

Searches of mobile phone or personal devices will only be carried out in accordance with our policy. See www.gov.uk/government/publications/searching-screening-and-confiscation)
Learners mobile phones or devices may be searched by a member of the leadership team, with the consent of the learner or a parent/carer. Content may be deleted or requested to be deleted, if it contravenes our policies.
Mobile phones and devices that have been confiscated will be released to parents or carers at the end of the day – or at the earliest next opportunity.

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.

Visitors use of personal devices and mobile phones

Parents/carers and visitors (including volunteers and contractors) must use their mobile phones and personal devices in accordance with our whole school safeguarding policy
Members of staff are expected to challenge visitors if they have concerns and will always inform the DSL (or deputy) or Head Teacher of any breaches our policy.

Officially provided mobile phones and devices

Members of staff will be issued with a work phone number and email address, where contact with learners or parents/ carers is required.

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

Setting mobile phones and devices will always be used in accordance with the acceptable use policy and other relevant policies including school personnel code of conduct.

All other rules relating to use of technology apply to setting mobile phones and devices.

Responding to Online Safety Incidents and Concerns

All members of the community will be made aware of the reporting procedure for online safety concerns, including: breaches of filtering, youth produced sexual imagery (sexting), cyberbullying and illegal content.

All members of the community follow the official procedures for reporting concerns as described in our whole school safeguarding policy.

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 to resolve online safety issues. After any investigations are completed, we 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 deputy) will seek advice from the Local Authority.

Where there is suspicion that illegal activity has taken place we will contact Norfolk Police using 101, or 999 if there is immediate danger or risk of harm.
If an incident or concern needs to be passed beyond our community (for example if other local settings are involved or the public may be at risk), the DSL or Head Teacher will speak with the Police and/or the Local Authority first to ensure that potential investigations are not compromised.

Concerns about learners welfare

The DSL (or deputy) will be informed of any online safety incidents involving safeguarding or child protection concerns.

The DSL (or deputy) will record these issues in line with our Whole School Safeguarding policy.
The DSL (or deputy) will ensure that online safety concerns are escalated and reported to relevant agencies in line with the Norfolk Safeguarding Children Board thresholds and procedures.

We will inform parents and carers of online safety incidents or concerns involving their child, as and when required.

Staff misuse

Any complaint about staff misuse will be referred to the Headteacher, in accordance with the safeguarding policy in relation to allegations against school staff.
Any allegations regarding a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer).
Appropriate action will be taken in accordance with our staff behaviour policy/code of conduct and safeguarding policy (allegations against staff).

Procedures for Responding to Specific Online Incidents or Concerns

Online sexual violence and sexual harassment between children

Our setting has accessed and understood "Sexual violence and sexual harassment between children in schools and colleges" (2018) This guidance was withdrawn in September 2022 and now forms part of Keeping Children Safe in Education.

Future Education recognises that sexual violence and sexual harassment between children can take place online. Examples may include; non-consensual sharing of sexual images and videos, sexualised online bullying, online coercion and threats, unwanted sexual comments and messages on social media, and online sexual exploitation. Full details of how we will respond to concerns relating to sexual violence and sexual harassment between children can be found within our Whole School Safeguarding Policy and anti-bullying policy.

Future Education recognises that internet brings the potential for the impact of any sexual violence and sexual harassment concerns to extend further than the local community, and for a victim or alleged perpetrator to become marginalised and excluded by online communities.

Future Education also recognises the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.

Future Education will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of online sexual violence and sexual harassment between children by implementing a range of age and ability appropriate educational methods as part of our PSHE and RSE curriculum.

We will ensure that all members of the community are aware of sources of support regarding online sexual violence and sexual harassment between children.

We will respond to concerns regarding online sexual violence and sexual harassment between children, regardless of whether the incident took place on our premises or using our equipment.

If made aware of online sexual violence and sexual harassment, we will:

- Immediately notify the DSL (or deputy) and act in accordance with our child protection and anti-bullying policies.
- If content is contained on learners electronic devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.
- Provide the necessary safeguards and support for all learners involved, such as offering specific advice on blocking, reporting and removing online content, as well as providing appropriate counselling/pastoral support.
- Implement appropriate sanctions in accordance with our behaviour policy.
- Inform parents and carers, if appropriate, about the incident and how it is being managed. If appropriate, make a referral to partner agencies, such as Children's Social Work Service and/or the Police.
- If the concern involves children and young people at a different educational setting, work in partnership with other DSLs to ensure appropriate safeguarding action is taken in the wider local community.
- If a criminal offence has been committed, the DSL (or deputy) will discuss this with the Police first to ensure that investigations are not compromised.
- Review the handling of any incidents to ensure that best practice was implemented, and policies/procedures are appropriate.

Youth produced sexual imagery (sexting)

Future Education recognises youth produced sexual imagery (known as "sexting" and 'sharing nudes or semi nudes') as a safeguarding issue; all concerns will be reported to and dealt with by the DSL (or deputy).

Future Education will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of 'sexting' by implementing preventative approaches, via a range of age and ability appropriate educational methods.

We will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery.

We will respond to concerns regarding youth produced sexual imagery, regardless of whether the incident took place on site or using setting provided or personal equipment. We will not:

- View any images suspected of being youth produced sexual imagery, unless there is no other possible option, or there is a clear need or reason to do so.
- If it is deemed necessary, the image will only be viewed by the DSL (or deputy DSL) and their justification for viewing the image will be clearly documented.
- Send, share, save or make copies of content suspected to be an indecent image of a child (i.e. youth produced sexual imagery) and will not allow or request learners to do so.

If made aware of an incident involving the creation or distribution of youth produced sexual imagery, we will:

- Act in accordance with our child protection policies and the relevant Norfolk Safeguarding Child Board's procedures.
- Ensure the DSL (or deputy) responds in line with the Local Authority and the Whole School Safeguarding Policy.

If an indecent image has been taken or shared on our network or devices, we will act to block access to all users and isolate the image.

- Carry out a risk assessment which considers any vulnerability of learners involved; including carrying out relevant checks with other agencies.
- Inform parents and carers, if appropriate, about the incident and how it is being managed.
- Make a referral to Children's Social Work Service and the Police.
- Provide the necessary safeguards and support for learners, such as offering counselling or pastoral support.
- Implement appropriate sanctions in accordance with our behaviour policy but taking care not to further traumatise victims where possible.
- Review the handling of any incidents to ensure that best practice was implemented; the leadership team will also review and update any management procedures, where necessary.

Online child sexual abuse and exploitation (including criminal exploitation)

Future Education will ensure that all members of the community are aware of online child sexual abuse, including: Exploitation and grooming; the consequences; possible approaches which may be employed by offenders to target children and how to respond to concerns.

Future Education recognises online child sexual abuse and exploitation (including criminal exploitation) as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the DSL (or deputy).
We will implement preventative approaches for online child sexual abuse and exploitation (including criminal exploitation) via a range of age and ability appropriate education for learners, staff and parents/carers.

We will ensure that all members of the community are aware of the support available regarding online child sexual abuse and exploitation (including criminal exploitation), both locally and nationally.

If made aware of incident involving online child sexual abuse and exploitation (including criminal exploitation), we will:

- Act in accordance with our child protection and safeguarding procedures and policies and the relevant Norfolk Safeguarding Child Board's procedures.
- If appropriate, store any devices involved securely. - Make a referral to Children's Social Work Service (if required/appropriate) and immediately inform Norfolk police via 101, or 999 if a child is at immediate risk.

- Carry out a risk assessment which considers any vulnerabilities of learner(s) involved (including carrying out relevant checks with other agencies).

Inform parents/carers about the incident and how it is being managed. o Provide the necessary safeguards and support for learners, such as, offering counselling or pastoral support.

Review the handling of any incidents to ensure that best practice is implemented; leadership team will review and update any management procedures, where necessary.

We will respond to concerns regarding online child sexual abuse and exploitation (including criminal exploitation), regardless of whether the incident took place on our premises or using setting provided or personal equipment. Where possible, learners will be involved in decision making and if appropriate, will be empowered to report concerns

If we are unclear whether a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through Norfolk Police.

If learners at other setting are believed to have been targeted, the DSL (or deputy) will alert the DSL at the setting involved and seek support from Norfolk Police.

Indecent images of children (IIOC)

Future Education will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC).

We will respond to concerns regarding IIOC on our equipment and/or personal equipment, even if access took place off site.

If we are unclear if a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through Norfolk Police and/or the Education Safeguarding Team.

If made aware of IIOC, we will: Act in accordance with our child protection policy and the relevant Norfolk Safeguarding Child Boards procedures.

- Store any devices involved securely.
- Immediately inform appropriate organisations, such as Norfolk police or the LADO.

If made aware that a member of staff or a learner has been inadvertently exposed to indecent images of children, we will:

- Ensure that the DSL (or deputy) is informed. Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
- Ensure that any copies that exist of the image, for example in emails, are deleted.
- Report concerns, as appropriate to parents and carers.

If made aware that indecent images of children have been found on the setting provided devices, we will:

- Ensure that the DSL (or deputy) is informed.
- Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
- Inform the police via 101 (999 if there is an immediate risk of harm) and Children's Social Work Service (as appropriate).
- Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only.
- Report concerns, as appropriate to parents and carers.

If made aware that a member of staff is in possession of indecent images of children on setting provided devices, we will:

- Ensure that the Headteacher is informed in line with our managing allegations against staff policy.

- Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with our managing allegations against staff policy.
- Quarantine any devices until police advice has been sought.

Online hate

Online hate content, directed towards or posted by, specific members of the community will not be tolerated at Future Education and will be responded to in line with existing policies, including antibullying and behaviour.
All members of the community will be advised to report online hate in accordance with relevant policies and procedures.
The Police will be contacted if a criminal offence is suspected.
If we are unclear on how to respond, or whether a criminal offence has been committed, the DSL (or deputy) will obtain advice through the Education Safeguarding Team and/or Norfolk Police.

Online radicalisation and extremism

We will take all reasonable precautions to ensure that learners and staff are safe from terrorist and extremist material when accessing the internet on site.
User access will be monitored as outlined earlier in this policy.

If we are concerned that a child or parent/carer may be at risk of radicalisation online, the DSL (or deputy) will be informed immediately, and action will be taken in line with our Safeguarding Policy and associated local safeguarding board guidelines and government guidelines on preventing radicalisation and extremism https://www.gov.uk/government/publications/preventingextremism-inschools-andchildrensservices/preventingextremism-in-the-education-and-childrensservicessectors

If we are concerned that member of staff may be at risk of radicalisation online, the Headteacher will be informed immediately, and action will be taken in line with the child protection and allegations policies.

National Links and Resources for Parents/Carers

- Action Fraud: www.actionfraud.police.uk •
- CEOP: www.thinkuknow.co.uk owww.ceop.police.uk
- Childnet: www.childnet.com
- Get Safe Online: www.getsafeonline.org
- Internet Matters: www.internetmatters.org
- Internet Watch Foundation (IWF): www.iwf.org.uk
- Lucy Faithfull Foundation: www.lucyfaithfull.org
- NSPCC: www.nspcc.org.uk/onlinesafety o ChildLine: www.childline.org.uk o Net Aware: www.netaware.org.uk
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk • UK Safer Internet Centre: www.saferinternet.org.uk

Headteacher:	Debbie Edwards	Date:	October 2026
Chair of Governing Body:	Daniel Childerhouse	Date:	October 2026