FARCET C. of E. PRIMARY SCHOOL

Online Safety POLICY

'Let your Light Shine' (Matthew 5:16)

Date Agreed: September 2025

Date for Review: September 2026

This policy, having been presented to, and agreed upon by the whole staff and Governors, will be distributed to:

- All staff
- School Governors
- Parents and Families of Farcet C. of E. Primary School

A copy of the policy will also be available in:

- The staffroom
- The school website

Contents

1. Our School Vision

Our school vision, 'Let Your Light Shine' (Matthew 5:16), underpins our aim for ensuring online safety in our school.

2. Aims

This policy takes into account the Department for Education's (DfE's) statutory safeguarding guidance, *Keeping Children Safe in Education (2025),* and its advice for schools on:

- Teaching online safety in schools: Teaching Online Safety in Schools (DfE, 2023).
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff. Cyber-bullying(DfE, 2014)
- Relationships, sex education and health education: Relationships, sex education and health education (DfE, 2025)
- Searching, screening and confiscation: Searching, Screening and Confiscation (DfE, 2022)

It also refers to the DfE's 2023 guidance on protecting children from radicalisation (Protecting children from radicalisation) It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyberbullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the KS1 and KS2 National Curriculum computing programmes of study.

3. Purpose of the policy

The purpose of Farcet CofE Primary School online safety policy is to:

- Safeguard and protect all members of Farcet CofE Primary School community online.
- Identify approaches to educate and raise awareness of online safety throughout the Farcet CofE Primary School community.
- Enable all staff to work safely and responsibly, to role model positive behaviour online and to manage professional standards and practice when using technology.
- Identify clear procedures to use when responding to online safety concerns.

4. Areas of Risk

Farcet CofE Primary School identify that the issues classified within online safety are considerable, but can be broadly categorised into four areas of risk. These are:

- **Content:** being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism.
- **Contact:** being subjected to harmful online interaction with other users, such as peer to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and;
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

5. Policy Scope

At Farcet CofE Primary School, we believe that:

- Online safety is an essential part of safeguarding and we acknowledge our duty to ensure that all pupils and staff are protected from potential harm online.
- The internet and associated devices, such as computers, tablets, mobile phones, smart watches and games consoles, are an important part of everyday life.
- Pupils 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 local governing body, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for DEMAT, or provide services on behalf of the school (collectively referred to as 'staff 'in this policy), as well as pupils, plus parents.

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

6. Educating Pupils about Online Safety

At Farcet CofE Primary School, we recognise the importance of educating our pupils in online safety. This is why we have established and embedded a progressive online safety curriculum throughout the whole school, to raise awareness and promote safe and responsible online use amongst pupils by:

1. Ensuring education regarding safe and responsible use precedes internet access.
2. Including online safety in the PSHE, SRE and Computing programmes of study, covering use both at school and home.
3. Reinforcing online safety messages whenever technology or the internet is in use.
4. Educating pupils in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation.

5. Teaching pupils to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

At Farcet CofE Primary School, to support pupils with this, we have created Acceptable Use Posters (AUPs) that have been written specifically for the age of the pupils so that they understand the content (Please see Appendix 1 for examples of AUPs). We reinforce the content of the age appropriate AUPs by:

- Displaying acceptable use posters in all classrooms.
- Informing pupils that network and internet use will be monitored for safety and security purposes and in accordance with legislation.
- Using support, such as external visitors, where appropriate, to complement and support the schools' internal online safety education approaches.

Pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private.
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.
- Use technology safely, respectfully and responsibly.
- Recognise acceptable and unacceptable behaviour.
- Identify a range of ways to report concerns about content and contact.

By the end of Year 6, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not.
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online, including when we are anonymous.

- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them.
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met.
- How information and data is shared and used online.
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context).
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know.

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 (where applicable) .

7. Educating and Training Staff

At Farcet CofE Primary School, we will:

- Provide all new staff members of staff with training, as part of their induction, on safe internet use and online safeguarding issues, including cyber-bullying and the risks of online radicalisation.
- All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails and staff meetings). This will cover the potential risks posed to pupils (Content, Contact, Conduct and Commerce) as well as our professional practice expectations.

- Make staff aware that school systems are monitored and activity can be traced to individual users; staff will be reminded to behave professionally and in accordance with school's policies when accessing school systems and devices.
- Make staff aware that their online conduct out of school, including personal use of social media, could have an impact on their professional role and reputation within school.
- Highlight useful educational resources and tools which staff should use, according to the age and ability of the pupils.
- Ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting pupils, colleagues or other members of the school community.

Through staff training, all staff will be made aware that technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse and/or cyber-bullying.

8. Awareness and Engagement with Parents

At Farcet CofE Primary School, we recognise that parents have an essential role to play in enabling children to become safe and responsible users of the internet and associated technologies. We also understand that technology and pupils knowledge of rapidly changes. Therefore, at Farcet CofE Primary School, we will build a partnership approach to online safety with parents by:

- Providing information and guidance on online safety in a variety of formats. This will include offering specific online safety awareness training and highlighting online safety at other events such as parent evenings and transition events.
- Drawing their attention to the school online safety policy and expectations in newsletters, letters, our school prospectus and on our school website.

- Requesting that they read online safety information as part of joining our school, for example, within our Home School Agreement.
- Requiring them to read the school AUP and discuss its implications with their child/children.
- Be aware of what systems the school uses to filter and monitor online use.
- Be aware of what their children are being asked to do online, including the sites they will be asked to access for homework.

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the Headteacher/Lead DSL and/or the Deputy Head/Deputy DSL.

9. Reducing Online Risks

At Farcet CofE Primary School, we recognise that the internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace therefore 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 school 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 a school computer or device.
- All members of the school community are made aware of the school's 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.

- Staff will receive training annually.
- Our website has a direct link to Child Exploitation and Online Protection where concerns about online sexual abuse or the way someone has been communicating with you online can be instantly reported.
- Be aware of the use of AI and challenges in this area.

10. Safer Use of Technology Classroom Use

At Farcet CofE Primary School, we use a wide range of technology. This includes access to:

- Laptops, iPADS and other digital devices.
- Internet which may include search engines and educational websites.
- Email.

All school owned devices will be used in accordance with the school's AUP 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.

Children will engage in research and pupils will use age appropriate search tools.

11. Filtering and Monitoring

DEMAT have ensured that Farcet CofE Primary School has age and ability appropriate filtering and monitoring in place, to limit children's exposure to online risks. All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard pupils; effective classroom management and regular education about safe and responsible use is essential.

The school uses *Netsweeper*, which is controlled by the school's internet provider. This blocks sites which can be categorised as: pornography, racial hatred, extremism, gaming and sites of an illegal nature. A report is sent to the Headteacher/Lead DSL.

Managing Filtering Breaches:

Farcet CofE Primary School has a clear procedure for reporting filtering breaches:

- If pupils discover unsuitable sites, they will be required to turn off monitor/screen and report the concern immediate to a member of staff.
- The member of staff will report the concern (including the URL of the site if possible) to the Lead DSL or Deputy DSL.
- The breach will be recorded and escalated as appropriate to DEMAT technical staff by the Lead DSL/Deputy DSL(s).
- Parents/carers will be informed of filtering breaches involving their child by the Lead DSL/Deputy DSL(s).
- Any material that the school believes is illegal will be reported by the Lead DSL/Deputy DSL(s) immediately to the appropriate agencies, such as: CEOP, Report Harmful Content, or the Internet Watch Foundation.

Monitoring

The school will appropriately monitor internet use on all school owned or provided internet enabled devices. All users will be informed that use of school systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation, in line with KCSIE (2025).

Security and Management of Information Systems

DEMAT takes appropriate steps to ensure the security of our information systems, including:

- Virus protection being updated regularly.
- Not downloading unapproved software to work devices or opening unfamiliar email attachments.
- The appropriate use of user logins and passwords to access the school network.
- All users are expected to log off or lock their screens/devices if systems are unattended.
- Staff will undertake Smartlog cyber training as requested by DEMAT.

12. Managing the Safety of the School Website

Farcet CofE Primary School will ensure that information posted on the school website meets the requirements as identified by the Department for Education (DfE):

- The school 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 pupils' personal information will not be published on the school website; the contact details on the website will be the school address, email and telephone number.
- The administrator account for the school website will be secured with an appropriately strong password.
- The school will post appropriate information about safeguarding, including online safety, on the school website for members of the community.

13. Managing Email

- Access to Farcet CofE Primary school email systems will always take place in accordance with Data protection legislation and in line with other DEMAT policies.

- Spam or junk mail will be blocked and reported by the Computing Lead to the DEMAT technicians to report to the provider.
- School email addresses and other official contact details will not be used for setting up personal social media accounts.
- Members of the school community will immediately tell the Head Teacher if they receive offensive communication, and this will be recorded in the school safeguarding files/records.

Staff

The use of personal email addresses by staff for any official school business is not permitted. All members of staff are provided with a specific school email address, to use for all official communication.

Pupils

Pupils are provided with email accounts for educational purposes by the school. Pupils will sign an AUP annually and will receive education regarding safe and appropriate email etiquette before access is permitted.

14. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)

- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device.
- Making sure the device locks if left inactive for a period of time.
- Not sharing the device among family or friends.
- Installing anti-virus and anti-spyware software as requested by DEMAT.
- Keeping operating systems up to date by always installing the latest updates as requested by DEMAT.
- Staff members must not use the device in any way that would violate the school's terms of acceptable use.
- Work devices must be used solely for work activities.
- If staff have any concerns over the security of their device, they must seek advice from the Computing Lead and DEMAT technicians.

15. Social Media Expectations

The expectations' regarding safe and responsible use of social media apply to all members of the school 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 staff at Farcet CofE Primary School are expected to engage in social media in a positive, safe and responsible manner, at all times.
- All members of Farcet CofE Primary School 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.

- Concerns regarding the online conduct of any member of staff on social media, should be reported to the school and will be managed in accordance with our DEMAT and local school policies.
- Whilst we acknowledge that parents will use social media, and that they may choose, for example, to set up class or year group *WhatsApp* groups, these are not endorsed by Farcet CofE Primary School, and they should not be used as a forum for unsubstantiated or malicious content.

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 the school code of conduct.
- No member of staff should engage with children or parents through social media. Where staff members are also parents, they have a responsibility to be professional at all times in their communication with parents via group or individual messaging.

Reputation

- All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within Farcet CofE Primary School and DEMAT. Civil, legal or disciplinary action may be taken if they 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): 1) Setting the privacy levels of their personal sites as strictly as they can. 2) Being aware of location sharing services. 3) Opting out of public listings on social networking sites. 4) Logging out of accounts after use. 5) Keeping passwords safe and confidential. 6) Ensuring staff do not represent their personal views as that of the school.
- Members of staff are encouraged not to identify themselves as employees of either Farcet CofE Primary School or DEMAT on their personal social networking accounts. This is to prevent information on these sites from being linked with the school/DEMAT and also 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 with school, plus DEMAT 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 pupils and their family members or colleagues will not be shared or discussed on social media sites.
- Members of staff will notify the Headteacher immediately if they consider that any content shared on social media sites conflicts with their role in the school.

Communicating with pupils and parents and carers

- All members of staff are advised not to communicate with or add as 'friends' any current or past pupils or current or past pupils' family members via any personal social media sites, applications or profiles.
- Staff will not use personal social media accounts to make contact with pupils or parents, nor should any contact be accepted.
- Any communication from pupils and parents received on personal social media accounts will be reported to the Headteacher/Lead DSL.

Pupils' Personal Use of Social Media

- Safe and appropriate use of social media will be taught to pupils as part of an embedded and progressive education approach, via age appropriate sites and resources.
- The school is aware that many popular social media sites state that they are not for children under the age of 13. We will also recommend to parents that they do not allow their children to access sites which are not age appropriate.
- Any concerns regarding pupils' use of social media, both at home and at school, will be dealt with in accordance with existing school/DEMAT policies. Concerns will also be raised with parents/carers as appropriate by the Lead DSL/Deputy DSL(s), particularly when concerning underage use of social media sites or tools.

Pupils 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. Examples would include real/full name, address, mobile or landline phone numbers, school attended, other social media contact details, email addresses, full names of friends/family, specific interests and clubs.

- To only approve and invite known friends on social media sites and to deny access to others by making profiles private/protected.
- 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 and report concerns both within school and externally.

16. Mobile phones

Staff use

Staff should refer to Farcet CofE Primary School Mobile Phone use policy for further guidance.

Pupils' Use of Personal Devices and Mobile Phones

Pupils will be educated regarding the safe and appropriate use of personal devices and mobile phones and will be made aware of boundaries and consequences.

- Children should not bring mobile phones into school, unless they are in Years 5 and 6 and come to or go home from school alone.
- Pupil's mobile phones must be turned off when on any part of the school grounds.
- The school expects pupil's mobile phones to be handed into the class teacher who sends the phones to the school office at the beginning of the day. The office staff will deliver the pupils phones to the class teacher at the end of the school day.

- If a pupil breaches the school policy, the phone or device will be confiscated and will be held in a secure place.
- School staff may confiscate a pupil's mobile phone or device if they believe it is being used to contravene the school/DEMAT policies or could contain youth produced sexual imagery (sexting).
- Pupils' mobile phones or devices may be searched by a member of Senior Leadership Team with the consent of the pupil or a parent.
- Mobile phones and devices that have been confiscated will be released to parents/guardians over the age of 18.
- If there is suspicion that material on a pupil'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 and visitors (including volunteers and contractors) must use their mobile phones and personal devices in accordance with the school/DEMAT policies.
- Members of staff are expected to challenge visitors if they have concerns and will always inform the Headteacher of any breaches of school policy.

17. Responding to online safety concerns

- All members of the school community will be made aware of the reporting procedure for online safety concerns, including: breaches of filtering, youth produced sexual imagery (sexting), up-skirting, cyberbullying and illegal content.
- All members of the community must respect confidentiality and the need to follow the official school procedures for reporting concerns.

- Pupils, parents and staff will be informed of the school's complaints procedure and staff will be made aware of the whistleblowing procedure.
- The school requires staff, parents and pupils to work in partnership to resolve online safety issues.
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any policy or curriculum changes as required.
- If the Headeacher/Lead DSL is unsure how to proceed with an incident or concern, they will seek advice from the DEMAT Safeguarding Team.
- Where there is suspicion that illegal activity has taken place, the Headteacher/Lead DSL will contact the both DEMAT Safeguarding Team, Cambridgeshire County Council Safeguarding Team or Police using 101, or 999 if there is immediate danger or risk of harm.

Concerns about Pupils Welfare

- The Lead DSL/Deputy DSL(s) will be informed of any online safety incidents involving safeguarding or child protection concerns.
- The Lead DSL/Deputy DSLs will ensure that online safety concerns are escalated and reported to relevant agencies in line with thresholds and procedures.
- The school will inform parents and carers of any incidents or concerns involving their child, as and when required.

Staff Misuse

- Any complaint about staff misuse will be referred to the Headteacher.

- 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 the school and DEMAT policies.

Procedures for Responding to Specific Online Incidents or Concerns

Youth Produced Sexual Imagery or "Sexting"

- Farcet CofE Primary School recognises youth produced sexual imagery (known as "sexting") as a safeguarding issue; therefore, all concerns will be reported to and dealt with by the Lead DSL/Deputy DSLs.

Dealing with 'Sexting'

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

- Act in accordance with our Safeguarding and Child Protection Policy.
- Immediately notify the Headteacher (Lead DSL) or Deputy DSLs
- Store the device securely.
- If an indecent image has been taken or shared on the school network or devices, the school will take action to block access to all users and isolate the image.
- Carry out a risk assessment which considers any vulnerability of pupil(s) involved; including carrying out relevant checks with other agencies.
- Inform parents and carers, if appropriate, about the incident and how it is being managed.
- Notify DEMAT Safeguarding Team.

- Make a referral to Cambridgeshire County Council Children's Services and/or the Police, as appropriate.
- Provide the necessary safeguards and support for pupils.
- Implement appropriate sanctions in accordance with the school's Behaviour policy, but taking care not to further traumatise victims where possible.
- The school will take action regarding youth produced sexual imagery, regardless of whether the incident took place on/off school premises, using school or personal equipment.

The school will not:

- View any images suspected of being youth produced sexual imagery, unless there is no other possible option (child shows staff member voluntarily), or there is a clear need or reason to do so.
- In this case, the image will only be viewed by the Headteacher (Lead DSL) or Deputy DSLs together 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 children (i.e. youth produced sexual imagery) and will not allow or request pupils to do so.

Online Child Sexual Abuse and Exploitation

- The school will implement preventative approaches for online child sexual abuse via a range of age and ability appropriate education for pupils, staff and parents.
- The school will ensure that the 'Click CEOP' report button is visible on the school website, and available to pupils and other members of the school community.

Dealing with Online Child Sexual Abuse and Exploitation

If the school are made aware of incident involving online sexual abuse of a child, the school will:

- Act in accordance with the school's Safeguarding and child protection policy and the Cambridgeshire County Council Safeguarding Child Board's procedures.
- Immediately notify the Headteacher (Lead DSL) or Deputy DSLs.
- Store any devices involved securely.
- Inform the DEMAT Safeguarding Team.
- Immediately inform the police via 101 (or 999 if a child is at immediate risk).
- Carry out a risk assessment which considers any vulnerabilities of pupil(s) involved (including carrying out relevant checks with other agencies).
- Inform parents about the incident and how it is being managed.
- Make a referral to Cambridgeshire County Council Children's Services.
- Provide the necessary safeguards and support for pupils, such as, offering pastoral support.

Cyberbullying

Cyberbullying, along with all other forms of bullying, will not be tolerated and will be dealt with in line with the schools' Anti-bullying and Behaviour Policy and Safeguarding Policy. Farcet CofE Primary School uses this definition of Cyber-bullying:

Cyberbullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power.

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim. All staff will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training. The school also publishes information in safeguarding newsletters on cyber-bullying to parents so they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The Headteacher (Lead DSL) or Deputy DSLs will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

18. Generative artificial intelligence (AI)

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

Farcet CofE Primary School recognise 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 'deep-fakes', where AI is used to create images, audio or video hoaxes that look real. This includes deep-fake pornography: pornographic content created using AI to include someone's likeness. Farcet CofE Primary School will treat any use of AI to bully pupils in line with our Safeguarding and Child Protection Policy and Behaviour Policy . Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the school/DEMAT.

19. Misuse of technology

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour and acceptable use. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures / staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident. The school will consider whether incidents that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

Children can abuse their peers online through:

- Abusive, threatening, 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.

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 up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term.
- The DSLs will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.
- Governors will receive training on safe internet use and online safeguarding issues as part of their DEMAT safeguarding training.
- Volunteers will receive appropriate training and updates, if applicable.

20. Roles and Responsibilities

Headteacher

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

SLT

SLT 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 Code of Conduct and an Acceptable Use Policy (AUP) that covers acceptable use of technology.
- Ensure that suitable and appropriate filtering and monitoring systems are in place.
- Ensure that online safety is embedded within a progressive whole school curriculum, which enables all pupils to develop an age-appropriate understanding of online safety.

DSLs

DSL (Lead and Deputies) will:

- Supporting the Headteacher/Lead DSL in ensuring that staff understand this policy and that it is being implemented consistently throughout the school.
- Work with the Headteacher and local governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly.
- Work with the Headteacher, Computing Leader, DEMAT IT technicians and other staff, as necessary, to address any online safety issues or incidents.
- Take the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks.
- Work with the Computing Leader and DEMAT IT technicians to make sure the appropriate systems and processes are in place.

- Manage all online safety issues and incidents in line with the school's safeguarding and child protection policy.
- Ensure that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy.
- Ensure that any incidents of cyber-bullying are logged on CPOMS and dealt with appropriately in line with the school behaviour policy.
- Update and deliver staff training on online safety (Appendix 3 contains a self-audit for staff on online safety training needs).
- Liaise with other agencies and/or external services if necessary.
- Providing regular reports on online safety in school to the Headteacher and/or local governing board.
- This list is not intended to be exhaustive

Computing Leader

The computing leader will:

- Ensure all staff and volunteers read and understand this policy.
- Have responsibility for the day-to-day running of this policy.
- Talk/present to governors, staff and parents on the potential risks and benefits relating to online safety.
- Oversee the online safety curriculum teaching.
- Work with the Lead DSL and Deputy DSLs to ensure that current legislation and guidelines are reflected in daily practice.
- Update the AUPs annually and share with pupils, families and staff.
- Develop the role of the Digital Leaders in online safety.

This list is not intended to be exhaustive.

All staff and volunteers

All staff and volunteers will:

- Maintaining an understanding of this policy.
- Implementing this policy consistently.
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet, and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2).
- Knowing that the DSLs are responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing.
- Working with the DSLs to ensure that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'.

This list is not intended to be exhaustive.

DEMAT IT Technicians

DEMAT IT technicians will:

- Provide technical support and perspective to the Headteacher (Lead DSL) and Deputy DSLs, especially in the development and implementation of appropriate online safety policies and procedures.
- Implement appropriate security measures to ensure that the school's IT infrastructure/system is secure and not open to

misuse or malicious attack, whilst allowing learning opportunities to be maximised.

- Ensure that the schools' filtering and monitoring procedures are applied and updated on a regular basis on school devices and school networks, to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material.
- Report any filtering breaches to the Headteacher (Lead DSL) and Deputy DSLs, as well as, the school's Internet Service Provider or other services, as appropriate.
- Ensure that any safeguarding concerns, identified through monitoring or filtering breaches are reported to the Headteacher (Lead DSL), in accordance with the school's safeguarding procedures.
- Put in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices, which are reviewed and updated at least annually to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material.
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.
- Conducting a full security check and monitoring the school's ICT systems on a monthly basis.

Pupils

Pupils will:

- Engage in age appropriate online safety education opportunities.
- Read and adhere to the school AUPs.
- 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.

Parents

Parents will:

- Ensure their child has read, understood, agreed and adhere to the terms on acceptable use of the school's ICT systems and internet (Appendices 1 and 2).
- Support the school in their online safety approaches by discussing online safety issues with their children and reinforce appropriate, safe online behaviours at home.
- Role model safe and appropriate use of technology and social media.
- Notify a member of staff or the Headteacher of any concerns or queries regarding this policy.
- Abide by the schools' home-school agreement and/or AUPs.
- Identify changes in behaviour that could indicate that their child is at risk of harm online.
- Seek help and support from the school, or other appropriate agencies, if they or their child encounter risk or concerns online.
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

Monitoring and Review

This policy will be reviewed at least annually by the Computing Leader, Lead DSL and Deputy DSLs. We will ensure that we 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 Headteacher will be informed of online safety concerns, as appropriate.

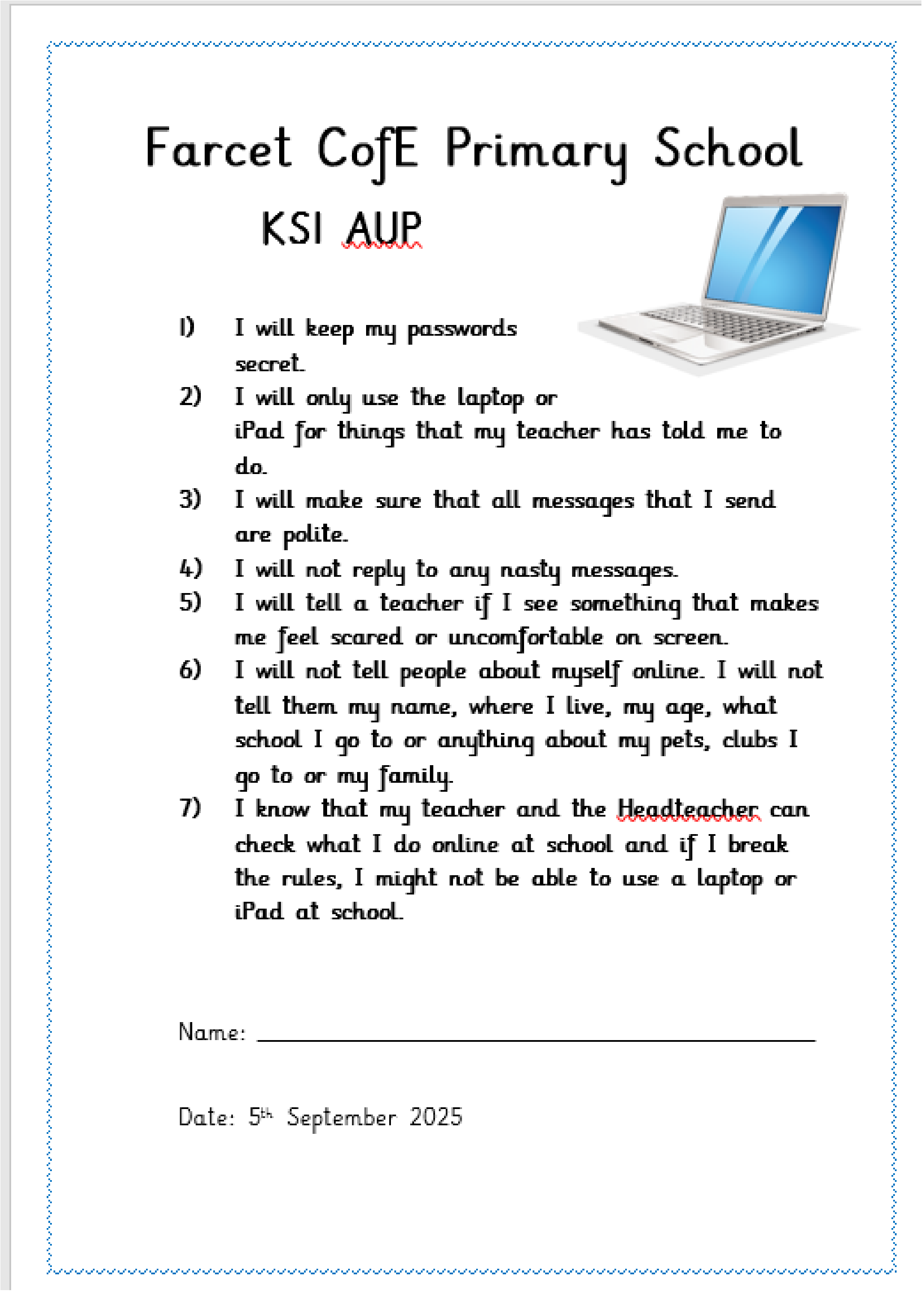
21. Useful Links for Educational Settings

National Links and Resources

- Action Fraud: https://www.actionfraud.police.uk/
- CEOP: https://www.ceopeducation.co.uk/
- Childnet: www.childnet.com
- Get Safe Online: https://www.getsafeonline.org/
- Internet Matters: https://www.internetmatters.org/
- Internet Watch Foundation (IWF): www.iwf.org.uk
- NSPCC: https://www.nspcc.org.uk/keeping-children-safe/online-safety/
- ChildLine: https://www.childline.org.uk/
- UK Safer Internet Centre: https://saferinternet.org.uk/
- Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline

Appendix 1

KS1 AUP



Farcet CofE Primary School

KS1 AUP

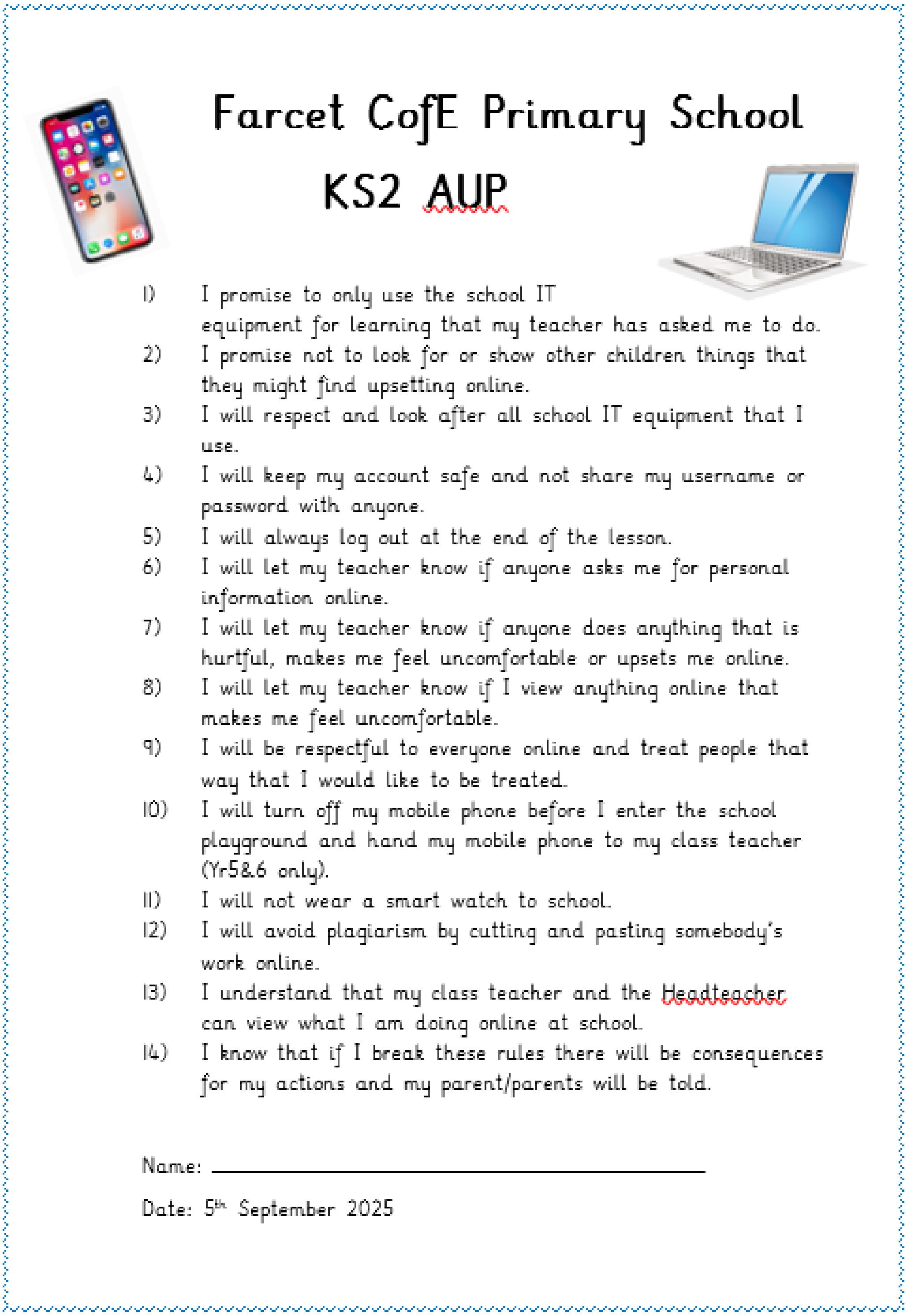
1) I will keep my passwords secret.
2) I will only use the laptop or iPad for things that my teacher has told me to do.
3) I will make sure that all messages that I send are polite.
4) I will not reply to any nasty messages.
5) I will tell a teacher if I see something that makes me feel scared or uncomfortable on screen.
6) I will not tell people about myself online. I will not tell them my name, where I live, my age, what school I go to or anything about my pets, clubs I go to or my family.
7) I know that my teacher and the Headteacher can check what I do online at school and if I break the rules, I might not be able to use a laptop or iPad at school.

Name: ___________________________________

Date: 5th September 2025

Appendix 2

KS2 AUP



Farcet CofE Primary School

KS2 AUP

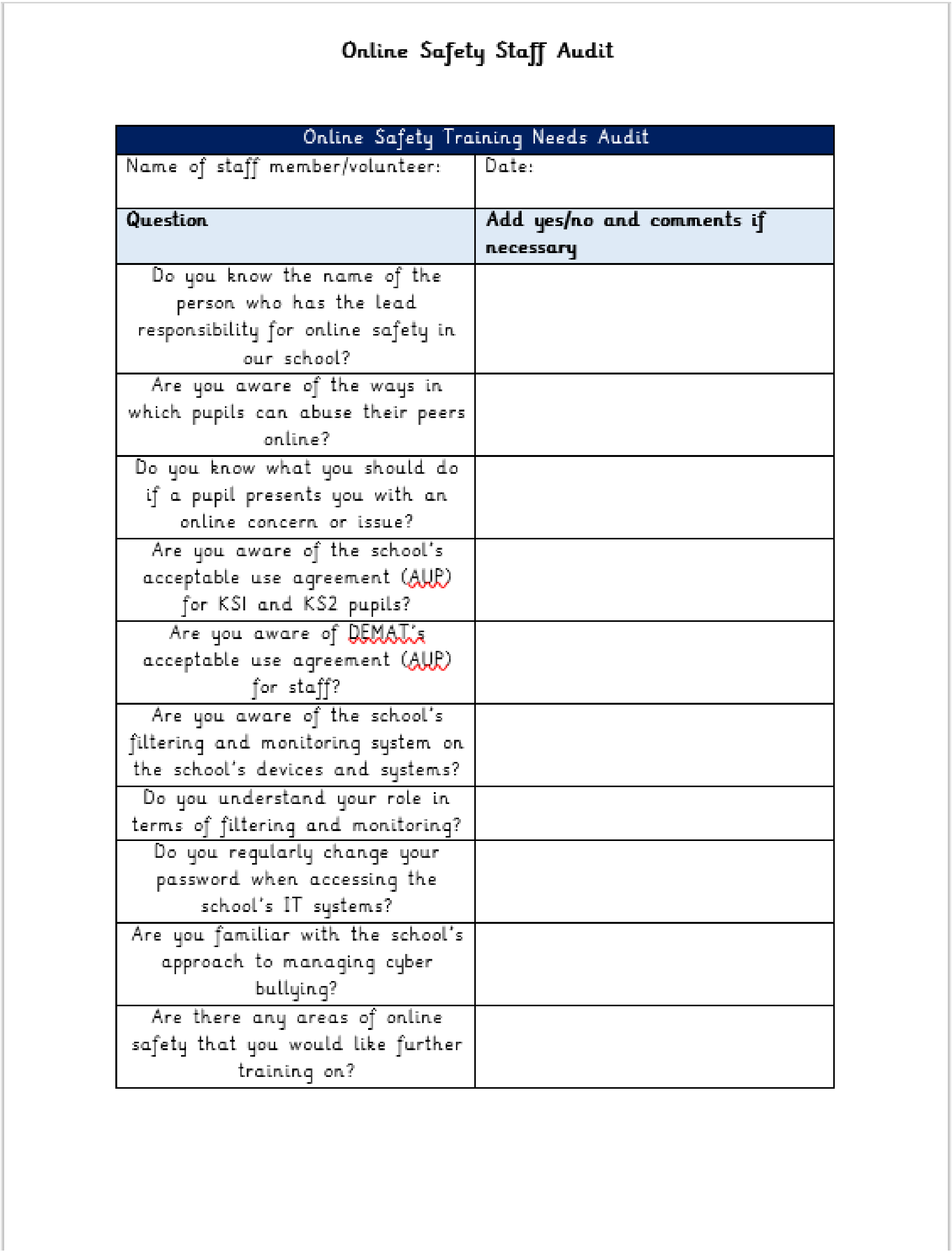
1) I promise to only use the school IT equipment for learning that my teacher has asked me to do.
2) I promise not to look for or show other children things that they might find upsetting online.
3) I will respect and look after all school IT equipment that I use.
4) I will keep my account safe and not share my username or password with anyone.
5) I will always log out at the end of the lesson.
6) I will let my teacher know if anyone asks me for personal information online.
7) I will let my teacher know if anyone does anything that is hurtful, makes me feel uncomfortable or upsets me online.
8) I will let my teacher know if I view anything online that makes me feel uncomfortable.
9) I will be respectful to everyone online and treat people that way that I would like to be treated.
10) I will turn off my mobile phone before I enter the school playground and hand my mobile phone to my class teacher (Yr5&6 only).
11) I will not wear a smart watch to school.
12) I will avoid plagiarism by cutting and pasting somebody's work online.
13) I understand that my class teacher and the Headteacher can view what I am doing online at school.
14) I know that if I break these rules there will be consequences for my actions and my parent/parents will be told.

Name: ____

Date: 5th September 2025

Appendix 3

Staff Audit



Online Safety Staff Audit

Online Safety Training Needs Audit	
Name of staff member/volunteer:	Date:
Question	**Add yes/no and comments if necessary**
Do you know the name of the person who has the lead responsibility for online safety in our school?	
Are you aware of the ways in which pupils can abuse their peers online?	
Do you know what you should do if a pupil presents you with an online concern or issue?	
Are you aware of the school's acceptable use agreement (AUP) for KS1 and KS2 pupils?	
Are you aware of DEMAT's acceptable use agreement (AUP) for staff?	
Are you aware of the school's filtering and monitoring system on the school's devices and systems?	
Do you understand your role in terms of filtering and monitoring?	
Do you regularly change your password when accessing the school's IT systems?	
Are you familiar with the school's approach to managing cyber bullying?	
Are there any areas of online safety that you would like further training on?	