SHINE
ACADEMIES

GROWMOOR SCHOOL & NURSERY

E-Safety Policy

October 2024

Rationale

As the use of online services and resources grows, so has awareness of the risks and potential dangers which arise from the use of communications technology and the internet. Those risks are not confined to the use of computers; they may also arise through the use of other handheld devices such as games consoles and mobile phones.

Children interact with new technologies on a daily basis. The exchange of ideas, social interaction and learning opportunities involved are greatly beneficial but can occasionally, if not used correctly, place children and young people in danger.

Our e-Safety Policy covers issues relating to children and young people and their safe use of the Internet, mobile phones and other electronic communications technologies, both in and out of school. It includes educating children on the risks and responsibilities of using such technologies safely and is part of the "duty of care" which applies to everyone working with children. Crowmoor Primary School and SHINE Academies will also provide safeguards and rules to guide staff, pupils and visitors in their online experiences.

e-Safety at Crowmoor Primary School and SHINE Academies is embedded in effective practice in each of the following areas:

- Education for responsible ICT use by all staff and pupils
- A comprehensive, agreed and implemented e-Safety Policy
- Use of a secure, filtered broadband and network
- A school network that complies with the National Education Network standards and specifications.

The policy is one of the strategies Crowmoor Primary School and SHINE Academies has in place to promote the safety of learners in their care both when they are in the school and when they are elsewhere.

Communications of this Policy

This e-Safety Policy has been written by the school, building on Local Authority and government guidance and through period of consultation with staff. It will be approved by Governors and the School Leadership Team. This policy will be available on the school's website and has been read and acknowledged by all staff.

Parents will be made aware that the school has a policy on e-Safety and will be advised on ways of keeping their children safe at home.

It is the responsibility of all staff to ensure that they use communications technology and the internet safely and responsibly. To this end, all staff and students agree to an Acceptable Use Policy (AUP).

Introducing the e-Safety Policy to pupils:

- e-Safety rules will be posted in all rooms where computers are used and discussed with pupils regularly.
- Pupils will be informed that network and Internet use will be monitored and appropriately followed up.
- e-Safety will be taught based on the materials from the Child Exploitation and Online Protection Centre (CEOP).
- e-Safety training will be embedded within the whole school curriculum.
- All children and young people require safe opportunities to understand the risks and benefits of the Internet and to balance these in their everyday use.

Staff and the e-Safety Policy:

- All staff will be given the School's e-Safety policy and emphasise its importance.
- Staff must be informed that network and Internet traffic can be monitored and traced to the individual user.
- Where appropriate, staff will always try use a child friendly, safe search engine when accessing the web with pupils e.g. "Yahoo Kids", "Kiddle" or "KidsSafeSearch".
- Regular e-Safety training will be part of the school's Continuing Professional Development (CPD) programme.

Parents and the e-Safety Policy:

- Parents' and carers' attention will be drawn to the school's e-Safety policy in newsletters, the school brochure/prospectus and on the school's website.
- The school will maintain a list of e-Safety resources for parents/carers which will be attached to the e-safety policy and available on the school website.
- e-Safety support, guidance, advice and/or workshops will be offered to parents/carers with an e-Safety support contact available on the school's website.

1.0 Internet Use in School

The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience.

The use of the internet and digital communications is a part of the statutory curriculum and a necessary tool for staff and pupils.

The purpose of Internet use at Crowmoor Primary School is to:

- Raise educational standards
- Promote achievements
- Support the professional work of staff
- Enhance management systems
- Provide information to parents and the wider community

Children also use the Internet regularly outside school to support their learning as well as for recreational reasons. The quality of the information received via the internet is variable. It is vitally important, therefore, for children to be taught the appropriate skills to select and evaluate internet content. It is also important that children know that they should report any unsuitable material to an adult immediately.

The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils via the SOPHOS filter.

e-Safety Actions

In the curriculum at Crowmoor Primary School, pupils will:

- Be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Be educated in the effective use of the Internet to research, including the skills of retrieval and evaluation.
- Be shown how to publish and present information to a wider audience.
- Be taught how to evaluate the relevance, accuracy and quality of Internet sourced material.
- Be taught the importance of cross-checking information before accepting its accuracy.
- Be supervised when using the Internet.
- Be taught how to report unpleasant Internet content by using the Child Exploitation and Online Protection Centre (CEOP) "Report Abuse" icon or similar systems.
- Know what to do if they experience any issues whilst online.
- Agree to an Acceptable Use Policy (AUP).

The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. The school cannot accept liability for the material accessed, or any consequences resulting from Internet use.

2.0 Managing Internet & Network Access

a. Information system security:

It is important that a school reviews and maintains the security of the whole computer and ICT system. This ensures the on-going delivery of essential learning services as well as the personal safety of staff and pupils. Maintaining computer security is a major responsibility of a school. It is a complex matter and will not be covered in full in this document. ICT infrastructure is monitored and controlled by S4S and their technicians.

e-Safety Actions

- The security of the school's information systems is reviewed regularly by the Computing Technicians, Computing Leader and Head Teacher.
- Virus protection is updated regularly.
- Use of the school purchased and accredited software ensures that all data sent by email is secure and all data stored on the platform is secure.
- Files held on the school's network are regularly checked and modified or deleted when necessary.
- Managing filtering:
    - The school will work with the Local Authority and a managed filtering system to ensure systems in place to protect pupils are reviewed and improved.
    - If staff or pupils come across unsuitable on-line materials, the site must be reported to the Computing Lead or the Head Teacher.
    - Children are taught to cover the device immediately when any unsuitable material appears, and notify an appropriate adult.
    - Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

b. Communication Software (email, TEAMS):

Email is an essential means of communication for both staff and pupils however the implications of email use in school need to be thought through and appropriate measures put in place. E-mails can be difficult to monitor but unregulated e-mail can leave pupils exposed to influences outside what is acceptable in school. Children will therefore have restricted access to many communicative aspects and devolved to curriculum teaching.

With the advancement of Microsoft TEAMS as a result of remote learning, children will have access to a communal chat area with staff. Chat features between children are disabled. See the Remote Learning Policy for more in depth details and procedures.

e-Safety Actions

- Children only use their Microsoft TEAMS and portal accounts.
- Pupils will be given a username and password to use the Office portal software as licensed by SHINE Academies.
- Children tell an adult immediately if they receive any offensive messages.
- Children do not reveal personal details about themselves or others when communicating online or arrange to meet with a specific person.
- The Computing Lead and SLT have access to all TEAMS for monitoring purposes.

c. Published content and the school website:

Crowmoor Primary School will regularly publish information, resources and children's outcomes on the school's management system, website and on social media accounts.

Personal information should only be held on secure systems which are accessed by authorised staff whereas general information about the school may be published wider. Our schools' website is an effective way of publishing information relevant to Crowmoor Primary School and SHINE Academies families and community, as it requires authentication while reaching a wide and relevant audience. In these cases consideration of personal and school security is essential and must be performed in accordance with the school's GDPR policy.

e-Safety Actions

- The only contact details on the website are the office e-mail and telephone number. Staff and children's information is not shared.
- The Head Teacher has overall editorial responsibility for the website to ensure that content is accurate and appropriate.
- Parents or carers give explicit written permission for images of children and their work to be posted on the website, pupil and family portals unless individual pupils cannot be clearly identified.

d. Social networking and personal publishing:

Parents and teachers need to be aware that the Internet has online spaces and social networking sites which allow children to publish content (e.g. photos, comments and personal information). These sites should only be viewed by invited 'friends'. All staff should amend settings to ensure their status and photos cannot be shared by anyone, by using networking sites permissions settings.

When used by responsible adults, social networking sites provide easy to use free facilities however children should be encouraged to think about the issues related to uploading personal information before signing up to social networking. Children are discouraged from signing up to online spaces or social networking sites.

e-Safety Actions

- The school blocks access to general social networking sites.
- Children are taught about the dangers (including bullying) of sharing personal information, especially online.
- Staff who use social networking sites must be aware of the nature of what they are publishing online in relation to their professional position.
- If staff are signed up to social networking sites, they must not discuss any matters relating to the school, children or their professional role online.
- Staff do not invite children to be 'friends' online and equally do not accept requests for friendship from children or past pupils of the school. Names of children requesting are passed onto the Head Teacher for further investigation.
- Where necessary, the school will closely control access to and the use of school accepted social networking sites, with consideration given as to how the pupils can be educated in their safe usage.
- Pupils and staff will be advised never to give out personal details of any kind which may identify them, their friends or their location.
- Pupils will be taught not to meet anyone first met online without specific permission or a responsible adult present.
- Pupils are encouraged to only ever use moderated social networking sites.
- Pupils and parents will be strongly advised of age restrictions of social networking sites that the use of social network spaces outside school may bring a range of dangers to all pupils.
- Ground rules must be established with pupils prior to video-conferencing to ensure appropriate behaviour. (see the Remote Learning Policy)
- Pupils must ask permission from the supervising teacher before making or answering a videoconference call. (see the Remote Learning Policy)
- Video-conferencing and webcam use will be appropriately supervised for the pupils' age. (see the Remote Learning Policy)

e. Managing emerging technologies:

Many emerging communications technologies offer the potential to develop new teaching and learning tool, including mobile communications and multimedia. A risk assessment needs to be undertaken on each new technology before using it with children. The safest approach is to deny access until a risk assessment has been completed and safety demonstrated. **e-Safety Actions**

- Emerging technologies are examined for educational benefit and a risk assessment will be carried out before use in school is permitted.
- If mobile phones are brought into school by children for safety purposes getting to and from school, they are placed in an agreed location for the duration of the child's school day and then returned at the end of the school day.
- Personal mobiles and personal digital cameras should not normally be used to record sound and images during the school day unless given permission by the Head Teacher.
- The senior leadership team should note that technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new access route to undesirable material and communications.
- When mobile technology is used in the classroom, clear ground rules must be established for its safe and appropriate use.
- School digital cameras or tablets are not to be taken off the school site (with the exception of school trips).
- Any photographs or videos taken on any handheld devices are to be used in school for educational purposes only, or to create a record of children's activities for use in class or to be uploaded onto the website. Once photographs or videos are downloaded from a handheld device, they will be deleted from that device. In particular, any handheld devices which are taken off school premises, must be cleared of school photos before being removed. Any stored media must be done so in line with the school's GDPR policy and located on the Media Drive (:M/)
- The appropriate use of Learning Platforms and collaborative software will be reviewed as the technology becomes available within the school.
- Pupils will be given a username and password to access any software which is licensed and monitored by the school or SHINE Academies.
- The educational benefits of mobile technology will be encouraged but not misused.

f. Families and Community Use

The school values the need for Internet access to be made available at home for the children. In addition, access may be available through the school library, the local library, youth services, adult education centres and supermarkets.

e-safety Actions

- The school will liaise with the local authority and local organisations such as the police, to establish a common approach to e-safety in conjunction with the eSafety pledge
- Parents' and carers' attention will be drawn to the school's e-Safety policy in newsletters, the school brochure/prospectus and on the school's website.
- The school will maintain, and regularly update, a list of e-Safety resources for parents/carers.

- e-Safety support, guidance, advice and/or workshops will be offered to parents/carers with an e-Safety support contact available on the school's website.

3.0 Leadership in e-Safety

a. Data Protection

The quality and variety of data held on pupils, families and on staff is expanding quickly. While this data can be very useful in improving services, data could be mishandled, stolen or misused. The Data Protection Act 2018 ("the Act") and the General Data Protection Regulation (GDPR) Act 2018 gives individuals the right to know what information is handled properly. The Head Teacher is responsible for ensuring the Data Protection procedures are in place and for liaising with the DPO. **e-Safety Actions**

- Personal data will be recorded, processed, transferred and made available according to the current regulations.
- Staff will not store data related to children, families or school on a removable storage device.
- All devices ae tracked and encrypted to protect any data that is stored on them.

b. Complaints Procedure

Keeping in line with school policy, if a member of staff, child, parent or carer has a complaint relating to e-Safety, then it will be considered and prompt action will be taken following an immediate investigation.

e-Safety Actions

- Parents will be provided with advice via Family Liaison and through e-Safety meetings or workshops.
- Parents will be made aware of the schools e-Safety policy and the AUP agreements in place.
- The school liaises with local schools and organisations to establish a common approach to e-Safety.
- The school will offer parents and families advice on matters of e-Safety eg, social networking sites and monitoring child access at home.
- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Head Teacher.

- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures. (Appendix 1 displays a flowchart of responses to an incident of concern.)
- Pupils and parents will be informed of consequences for pupils misusing the Internet

c. Authorising Internet access e-safety Actions

- All staff must read and sign the Staff Acceptable Use Policy before using any school ICT resource.
- Any governors that use school technology must sign an acceptable use policy.
- All pupils are guided through an AUP as part of the curriculum.
- At Crowmoor Primary School and SHINE Academies, access to the Internet will be with adult supervision and will only access specific, approved on-line materials.

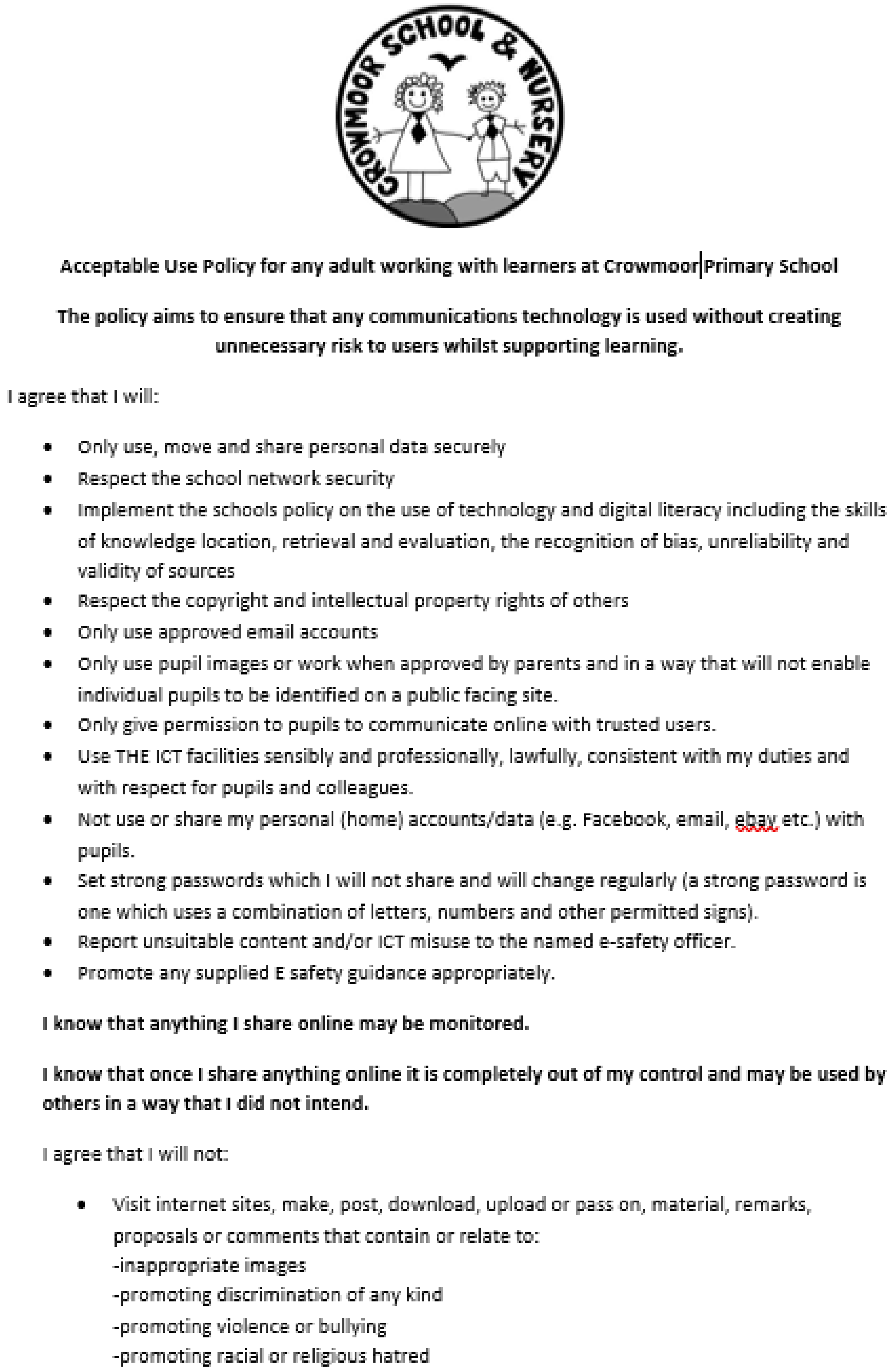
d. Assessing risks: e-safety Actions

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. Neither the school nor Local Authority can accept liability for any material accessed or any consequences of Internet access.
- The school will carry out an annual audit of ICT use to establish if the e-Safety policy is adequate and that the implementation of the e-Safety policy is appropriate and effective.

4.0 Monitoring & Review

This policy will be reviewed on an **annual** basis by the **SLT & Computing Lead.** Any changes to this policy will be communicated to all members of staff and other stakeholders. The next scheduled review date for this policy is September 2025

Appendix 1



Acceptable Use Policy for any adult working with learners at Crowmoor Primary School

The policy aims to ensure that any communications technology is used without creating unnecessary risk to users whilst supporting learning.

I agree that I will:

- Only use, move and share personal data securely
- Respect the school network security
- Implement the schools policy on the use of technology and digital literacy including the skills of knowledge location, retrieval and evaluation, the recognition of bias, unreliability and validity of sources
- Respect the copyright and intellectual property rights of others
- Only use approved email accounts
- Only use pupil images or work when approved by parents and in a way that will not enable individual pupils to be identified on a public facing site.
- Only give permission to pupils to communicate online with trusted users.
- Use THE ICT facilities sensibly and professionally, lawfully, consistent with my duties and with respect for pupils and colleagues.
- Not use or share my personal (home) accounts/data (e.g. Facebook, email, ebay etc.) with pupils.
- Set strong passwords which I will not share and will change regularly (a strong password is one which uses a combination of letters, numbers and other permitted signs).
- Report unsuitable content and/or ICT misuse to the named e-safety officer.
- Promote any supplied E safety guidance appropriately.

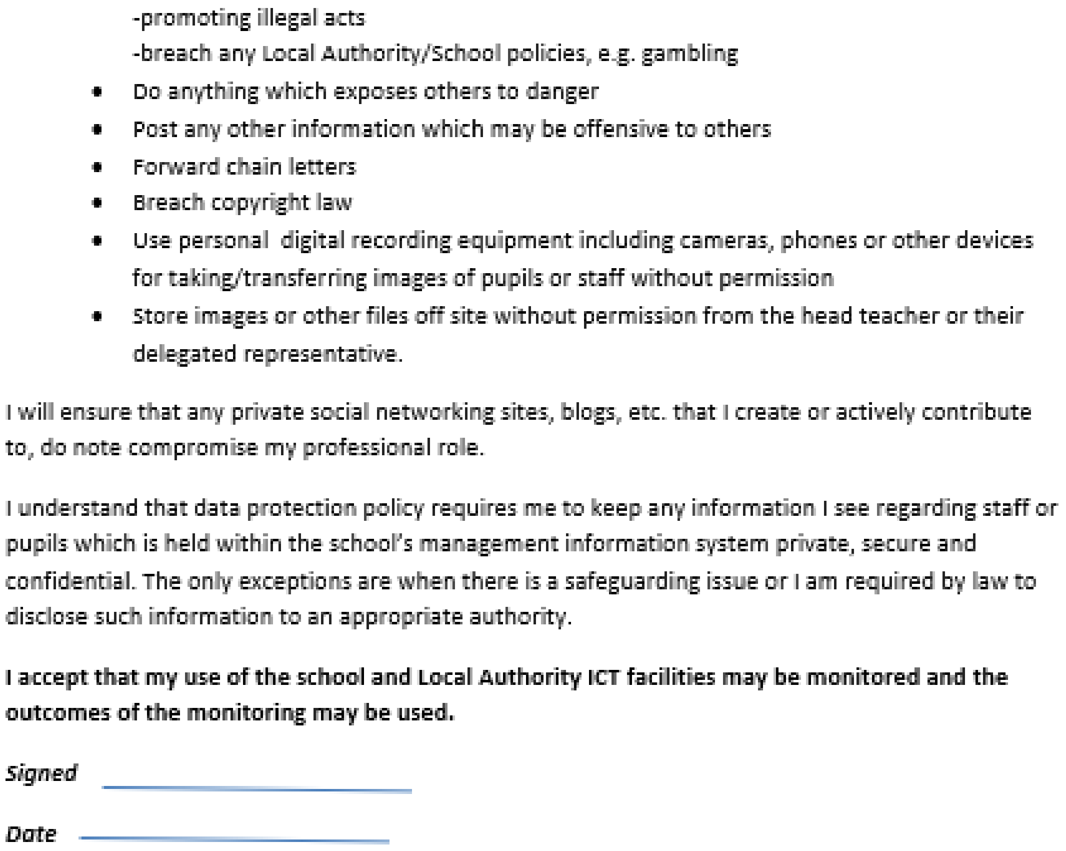
I know that anything I share online may be monitored.

I know that once I share anything online it is completely out of my control and may be used by others in a way that I did not intend.

I agree that I will not:

- Visit internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:
  -inappropriate images
  -promoting discrimination of any kind
  -promoting violence or bullying
  -promoting racial or religious hatred

Appendix 2



-promoting illegal acts
-breach any Local Authority/School policies, e.g. gambling

- Do anything which exposes others to danger
- Post any other information which may be offensive to others
- Forward chain letters
- Breach copyright law
- Use personal digital recording equipment including cameras, phones or other devices for taking/transferring images of pupils or staff without permission
- Store images or other files off site without permission from the head teacher or their delegated representative.

I will ensure that any private social networking sites, blogs, etc. that I create or actively contribute to, do note compromise my professional role.

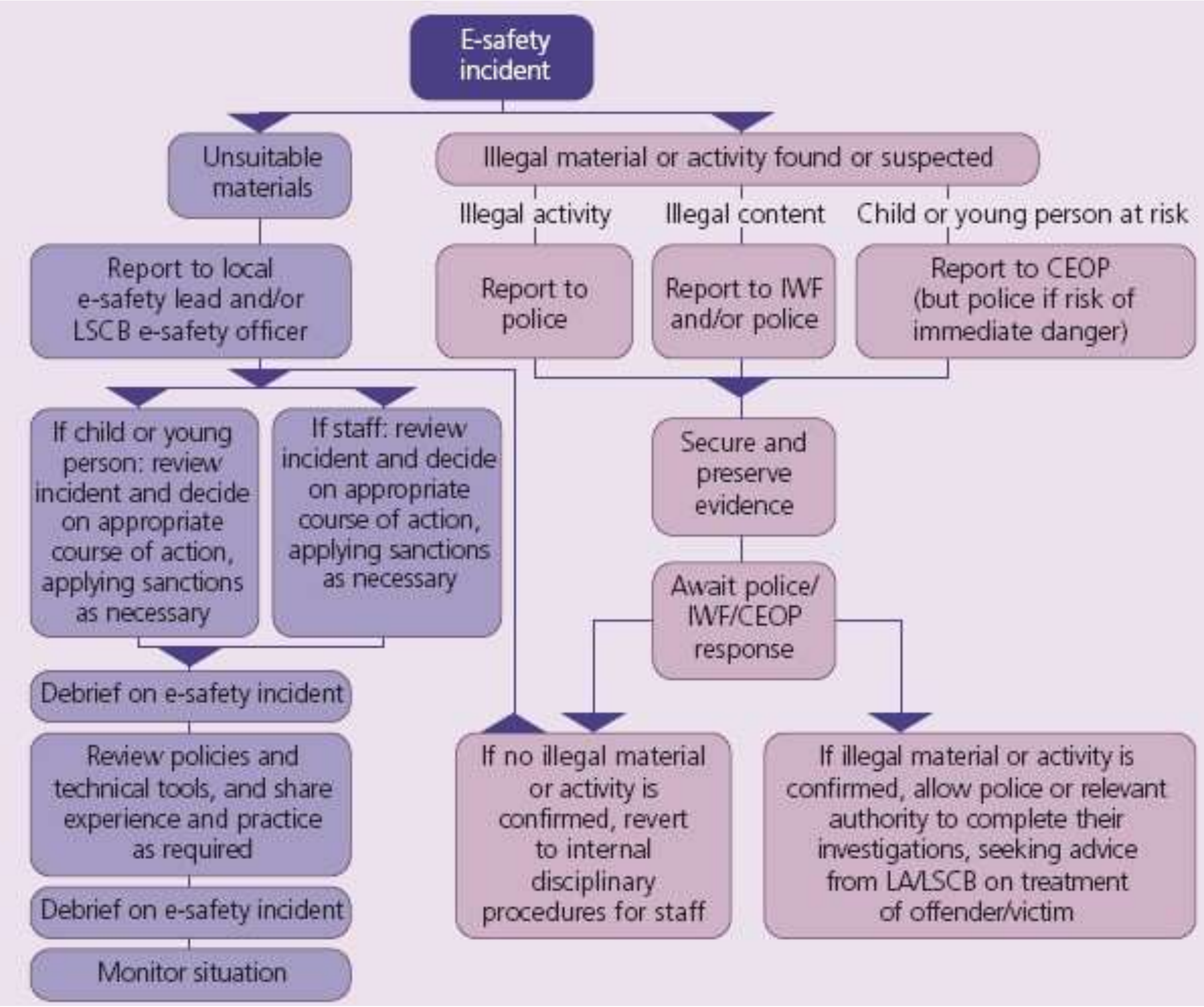
I understand that data protection policy requires me to keep any information I see regarding staff or pupils which is held within the school's management information system private, secure and confidential. The only exceptions are when there is a safeguarding issue or I am required by law to disclose such information to an appropriate authority.

I accept that my use of the school and Local Authority ICT facilities may be monitored and the outcomes of the monitoring may be used.

Signed ____________________

Date ____________________

Appendix 3


E-safety incident
Unsuitable materials
Illegal material or activity found or suspected
Illegal activity
Illegal content
Child or young person at risk
Report to local e-safety lead and/or LSCB e-safety officer
Report to police
Report to IWF and/or police
Report to CEOP (but police if risk of immediate danger)
If child or young person: review incident and decide on appropriate course of action, applying sanctions as necessary
If staff: review incident and decide on appropriate course of action, applying sanctions as necessary
Secure and preserve evidence
Await police/ IWF/CEOP response
Debrief on e-safety incident
Review policies and technical tools, and share experience and practice as required
Debrief on e-safety incident
Monitor situation
If no illegal material or activity is confirmed, revert to internal disciplinary procedures for staff
If illegal material or activity is confirmed, allow police or relevant authority to complete their investigations, seeking advice from LA/LSCB on treatment of offender/victim

(Figure reproduced from Becta - *Safeguarding children online: a guide for Local Authorities and Local Safeguarding Children Boards*, page 27, appendix B)

Appendix 4

SHINE Academies e-Safety Audit: Crowmoor Primary School

Has the school an e-Safety Policy in conjunction with SHINE Academies and Shropshire Local Authority?	Y
The school e-safety policy was agreed on: September 2024	
The policy is available for staff on: September 2024	
The policy is available for parents/carers: September 2024	
The responsible member of the Senior Leadership Team is: Head of School	
The responsible member of the Governing Body is: Chair of Governors	
The Designated Child Protection Officer is: Mr R Horton	
The e-Safety lead in school is: Miss B Jones	
Has e-safety training been provided for pupils?	Y – ongoing
Has e-safety training been provided for staff?	Y - ongoing
Is there a clear procedure for a response to an incident of concern?	Y
Have e-safety materials been obtained from recommended providers?	Y
Do all staff sign an Acceptable Use Policy on appointment?	Y
Are all pupils aware of the School's e-Safety rules and acceptable use policy?	Y
Are e-Safety rules or Acceptable Use Policies displayed in all rooms where computers are used and expressed in a form that is accessible to all pupils?	Y
Do parents/carers sign and return an agreement that their child will comply with the School e-Safety rules and acceptable use policy?	Y
Are staff, pupils, parents/carers and visitors aware that network and Internet use is closely monitored and individual usage can be traced?	Y
Has an ICT security audit been initiated by the Senior Leadership Team, possibly using external expertise?	Y
Is personal data collected, stored and used according to the principles of the Data Protection Act?	Y
Is Internet access provided by an approved educational Internet service provider which complies with Department for Education (DfE) requirements.	Y
Has the school-level filtering been designed to reflect educational objectives and approved by the Senior Leadership Team?	Y
Is anti-virus up-to-date, and installed on all devices?	Y
Are all shareholders aware of the CEOP Report Abuse button?	Y
Is there a working link on the School website to report abuse using the CEOP button?	Y

Appendix 5

Useful resources

Child Exploitation and Online Protection Centre: www.ceop.gov.uk

Childnet: www.childnet-int.org

Kidsmart: www.kidsmart.org.uk

Safer Children in the Digital World: www.dfes.gov.uk/byronreview

Think U Know: www.thinkuknow.co.uk

NSPCC: https://www.nspcc.org.uk/keeping-children-safe/online-safety/

Internet Watch Foundation: www.iwf.org.uk

Parents Centre: www.parentscentre.gov.uk

Internet Safety Zone: www.internetsafetyzone.com

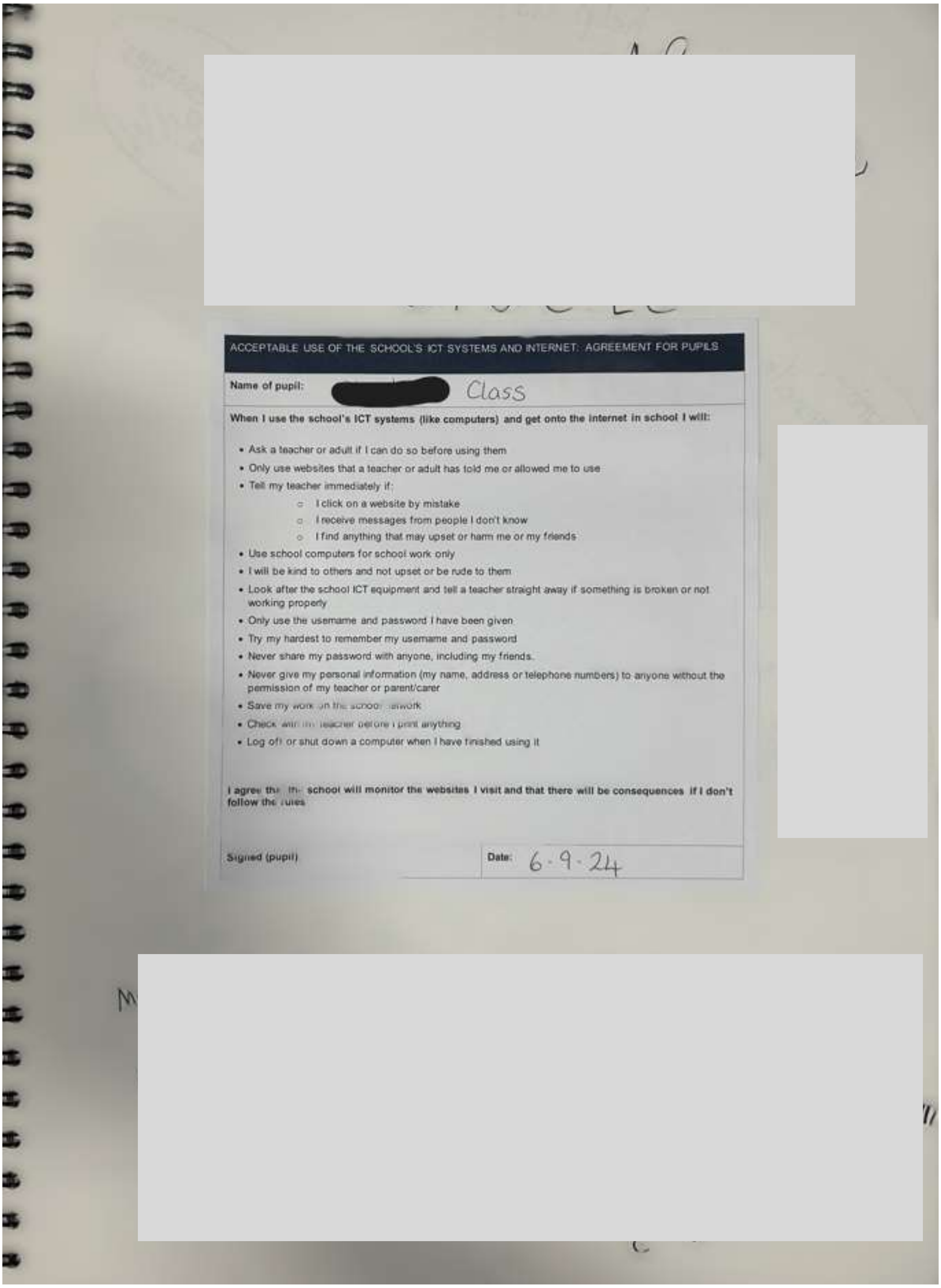
Safety Net Kids: http://www.safetynetkids.org.uk/personal-safety/staying-safe-online/

Childline: https://www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobilesafety/staying-safe-online/

National Online Safety: https://nationalonlinesafety.com/guides

Internet Matters: https://www.internetmatters.org/advice/6-10/

Acceptable Use Agreement



[redacted]

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

Name of pupil: [redacted] Class	

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

- Ask a teacher or adult if I can do so before using them
- Only use websites that a teacher or adult has told me or allowed me to use
- Tell my teacher immediately if:
  - I click on a website by mistake
  - I receive messages from people I don't know
  - I find anything that may upset or harm me or my friends
- Use school computers for school work only
- I will be kind to others and not upset or be rude to them
- Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly
- Only use the username and password I have been given
- Try my hardest to remember my username and password
- Never share my password with anyone, including my friends.
- Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer
- Save my work on the school network
- Check with my teacher before I print anything
- Log off or shut down a computer when I have finished using it

I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules

Signed (pupil):	**Date:** 6·9·24

[redacted]

[redacted]