# Amblecote Primary School

*'At Amblecote we achieve because in our pupils we believe.'*

# Online Safety Policy

**Responsibility for monitoring this policy: Head teacher and Online Safety Lead**

**Review: annually**

**(or in response to changes in legislation/LA operating procedures)**

**Reviewed: November 2023**

**Proposed by the Headteacher** J Cook **Mrs J. Cook**

**Approved by Governing Body** ..... **Mrs C. Roberts (Chair of Governors)**

**Purpose:**

**The purpose of this policy is to ensure the safe and responsible use of online platforms and technology within the school community. It aims to protect students, staff, and parents from potential risks associated with online activities, while promoting digital literacy and responsible digital citizenship.**

**School Leadership will**

- **Develop and review the online safety policy regularly.**
- **Provide necessary resources and training to staff, students, and parents.**
- **Ensure compliance with legislation and guidelines.**
- **Appoint an Online Safety Lead to oversee the implementation of the policy.**

Governors are responsible for reviewing the effectiveness of this policy. A member of the governing body is to take on the role of Online Safety Link Governor, whose role is to:

- Meet regularly with the school's Online Safety Lead
- Report to relevant Governor committees
- Have an overview of the latest developments in the school's information and communication systems, including records, monitoring procedures and data protection.

The Head teacher is responsible for ensuring the safety (including Online safety) of members of the school community. Day to day responsibility for Online safety is delegated to the Online Safety Lead (member of SLT) whose responsibilities include ensuring that:

- all staff are aware of the procedures on Online safety and are able to train other colleagues where relevant.
- pupils are taught how to use ICT tools such as the internet, e-mail and social networking sites safely and appropriately. The LA has provided Guidelines for the Use of Social Networks (**https://safeguarding.dudley.gov.uk/media/11658/social_networking.pdf**)
- there is a system in place to allow for monitoring and support for those in school who carry out the Online safety monitoring role. (**Appendix 1**)
- reports on Online safety incidents are made to DSL.
- Verbal reports are regularly made to SLT.
- Email to alert school of any Smoothwall incidents.
- The Head teacher, Online safety Lead and Child Protection Officer should be aware of the procedures to be followed in the event of a serious Online safety allegation being made against a member of staff. (**Appendix 1**)
- The Head teacher is responsible for ensuring that parents and carers, when given access to data and information relating to their child / children, via any cloud-based website, Learning Platform or Gateway, have adequate information and guidance relating to the safe and appropriate use of this online facility (The **Information Security Policy** contains more detailed guidance)

**Online Safety Lead will**

- **Stay updated with the latest online safety practices and legislation.**
- **Develop and deliver online safety training for staff, students, and parents.**

- **Monitor and evaluate the effectiveness of the policy.**
- **Collaborate with external agencies and organizations to enhance online safety measures.**

**Staff will**

- **Familiarize themselves with the online safety policy and guidelines.**
- **Promote safe and responsible use of technology among students.**
- **Report any online safety concerns to the designated Online Safety Lead.**

All teaching and support staff are responsible for ensuring that:

- They have an up-to-date awareness of Online Safety, matters and of the current Online safety policy.
- They encourage pupils to develop good habits and behaviours when using ICT to keep themselves, and others, safe.
- They have read, understood and agreed to the school's Staff Acceptable Use Policy (AUP) on an annual basis (**Appendix 3**)
- They report any suspected misuse or problem to the Online Safety Lead
- Digital communications with pupils using e-mail, through online Learning Environments or websites that offer dialogue and commenting functionality etc., should be on a professional level and only carried out using official school systems.
- Online safety issues are embedded in all aspects of the curriculum and other school activities.
- Pupils follow the Online safety and Acceptable Use Policy (**Appendix 4**)
- Pupils have an understanding of research skills and the need to avoid plagiarism and that they uphold copyright regulations.
- They are aware of Online safety issues and requirements related to the use of mobile phones, cameras and hand-held devices and that they monitor their use and implement the school's policy in regard to these devices.
- In lessons where internet use is pre-planned, pupils should be guided to sites which have been checked as suitable and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Staff act as good role models in their use of ICT, the internet and mobile devices.

The DSL are trained in Online safety issues and should be aware of the potential for serious child protection issues to arise from:

- Sharing of personal data
- Access to illegal or inappropriate materials
- Inappropriate online contact with adults or strangers
- Inappropriate online contact with known peers or adults
- Potential or actual incidents of grooming
- Cyber-bullying

Community users who access school ICT systems, the web site or any online Learning Environment as part of the extended school provision are expected to sign a Community User Acceptable Use Policy before being provided with access to the school's systems. In practice, access is very limited and is mainly only available to PGCE or GTP students who also sign the AUP (**Appendix 3**)

**Use of digital and video images**

- The school allows staff to bring in personal mobile phones and devices for their own use.

Only under certain circumstances should a member of staff contact a parent/carer using their personal device (e.g., to contact them whilst off site on a school visit)

- The school is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate text messages between any member of the school community is not allowed.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.
- The school provides a safe and secure way of using chat rooms, blogs and other 'social networking technologies' via the Learning Platform. Other 'social networking' facilities may be 'unfiltered' for curriculum purposes. Staff are aware of the procedure they need to follow when requesting access to externally based social networking sites (**https://safeguarding.dudley.gov.uk/media/11658/social_networking.pdf**)
- The school requests permission for the use of pupils' images on any published media. Lists of pupils for whom no permission has been given is kept on the teacher's area of the school network and should be consulted before using any images of pupils.

For full guidelines on the use of digital and video images, see **Policy on Use of Electronic Devices**

**Data Protection**

- Personal data is recorded, processed, transferred and made available according to the Data Protection Act 2018 which states that personal data must be:
  - Fairly and lawfully processed.
  - Processed for limited purposes.
  - Adequate, relevant and not excessive
  - Accurate
  - Kept no longer than is necessary.
  - Processed in accordance with the data subject's rights.
  - Secure
  - Only transferred to others with adequate protection
- Staff must be aware of the Information Security Policy. A breach of the Data Protection Act may result in the school or an individual fine.
- Staff must ensure that they:
  - Take care at all times, to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
  - Access personal data on secure password protected computers and other devices or via any online Learning Platform or SMIS ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
  - Transfer data using encryption and secure password protected devices.
- When personal data is stored on any portable computer system, USB stick or any other removable media:
  - The data must be encrypted, and password protected.
  - The device must be password protected *(many memory sticks / cards and other mobile devices cannot be password protected.)*

- The device must offer approved virus and malware checking software.
- The data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete.

**Students will**

- **Use technology and online platforms responsibly and ethically.**
- **Report any online safety concerns to a trusted adult or staff member.**
- **Follow school guidelines and rules regarding online activities.**

A planned and progressive Online safety programme is provided as part of ICT and across the curriculum and is regularly revisited – this includes the use of ICT and new technologies in school and outside school. Key Online safety messages are reinforced as part of a planned rolling programme of assemblies and class activities. Pupils are taught in all lessons to be critically aware of the materials and content they access online and are guided to validate the accuracy of information. Students and pupils are taught the importance of information security and the need to keep information such as their password safe and secure. Pupils have access to the school network and technologies what enable them to communicate with others beyond the school environment. The network is a secure system provided through DGfL.

It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g., racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the class teacher or managed service provider temporarily remove those sites from the filtered list for the period of study. Any requests to do so are auditable and should be logged.

Pupils:

- are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy (**Appendix 4**) which they are expected to agree to annually before being given access to school systems.
- pupils understand that there are sanctions for inappropriate use of technologies and the school will implement these sanctions in accordance with the acceptable use agreement.
- need to have a good understanding of research skills and the need to avoid plagiarism and to uphold copyright regulations.
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and that they know how to do so.
- Should understand that the school has a 'duty of care' to all pupils. The misuse of non-school provided systems, out of school hours, will be investigated by the school in line with our behaviour, anti-bullying and safeguarding policies.
- are expected to know and understand school policy on the use of electronic devices and should know and understand school policies on the taking / using of images, use of social networking sites and on cyber bullying (**https://safeguarding.dudley.gov.uk/media/11658/social_networking.pdf**)
- should understand the importance of adopting good Online safety practice and behaviours when using digital technologies out of school.
- Have the opportunity to become Digital leaders in Key Stage 2
- In Key Stage 2 are responsible for choosing an appropriate secure password and are reminded to change these regularly
- Children in UKS2 are educated about the dangers of 'sexting or youth produces sexual imagery' during RSE lessons.

**Parents will**

- **Support and reinforce online safety practices at home.**
- **Stay informed about the school's online safety policy and guidelines.**
- **Report any online safety concerns to the school.**

Parents and Carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in a safe and appropriate way. The school therefore takes every opportunity to help parents understand these issues through parents' evenings, assemblies, newsletters, letters, its website, and other information provided by national and local agencies, such as Childline and National Online Safety

Parents and Carers are responsible for:

- Accessing the school web site and any online pupil records in accordance with the Acceptable Use Policy **(Appendix 4**)

**Filtering and Monitoring will**

- **Implement appropriate filtering and monitoring systems to restrict access to harmful content.**
- **Regularly review and update filtering and monitoring systems to ensure effectiveness.**

**Managed Service Provider**

Smoothwall Monitoring and Safety is responsible for helping the school to ensure that it meets the Online safety requirements outlined by DGfL. The managed service provides a number of tools to schools including DGfL filtering tools, and monitoring solutions such as Smoothwall monitoring, which are designed to help keep users safe when online in school (**Appendix 2**).

The Managed Service Providers is responsible for ensuring that the school infrastructure and network is as safe and secure as is reasonably possible. Smoothwall Monitoring provides a weekly monitoring report to The Headteacher, Deputy Headteacher and DSL/Computing Lead) Smoothwall monitoring looks for trigger words and safeguarding concerns, a screenshot is taken and sent to human monitoring 24/7 day, 365 days a year. The school is responsible for ensuring that policies and procedures approved within this policy are implemented.

School ICT systems are managed in a way that ensures that the school meets the Online safety technical requirements outlined in the Acceptable Use Policies

- There will be regular reviews and audits of the safety and security of school ICT systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users have clearly defined access rights to school ICT systems.
- All users are provided with a username and password.
- Users will be made responsible for the security of their username and password. They must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- The school maintains and supports the managed filtering service provided by DGfL.
- The school manages and updates filtering issues through the RM helpdesk.

- Requests from staff for sites to be removed from the filtered list will be considered by the Online Safety Lead and Headteacher. If the request is agreed, this action will be recorded, and logs of such actions shall be recorded.
- Remote management tools are used by staff to control workstations and view users' activity.
- An appropriate system is in place for users to report any actual or potential Online safety incident to the relevant person.
- The managed service provider ensures that appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, mobile and/or handheld devices etc from accidental or malicious attempts which might threaten the security of the school systems and data
- An agreed procedure is in place regarding the use of removable media (e.g., memory sticks, email and cloud) by users on school workstations and portable devices.
- The school infrastructure and individual workstations are protected by up-to-date virus software.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

### 3.3 Staff Training

**Provide regular training sessions for staff on online safety practices and procedures.**

**Equip staff with the knowledge and skills to support students in navigating online risks.**

- Annually all staff receive statutory safeguarding updates, which includes online safety. All DSLs and staff receive training on filtering and monitoring.

### 3.4 Reporting Mechanisms will

- **Establish clear procedures for reporting online safety concerns.**
- **Ensure students, staff, and parents know how and to whom they should report any issues.**
- **Review Mechanisms**

When using communication technologies, the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Staff and students / pupils should therefore use only the school email service to communicate with others when in the school, or on school systems e.g., by remote access from home- (If staff use nonstandard or personal email accounts these are not secure and cannot always be monitored) The school also uses ClassDojo App to communicate two-way with parents however staff are aware that this is not monitored.
- Users need to be aware that email communications may be monitored.
- Users must immediately report to the nominated person – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.

- Any digital communication between staff and students / pupils or parents / carers (email, chat, ClassDojo etc.) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.
- Students / pupils are provided with individual school email addresses for educational use.
- Students / pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the school website, on public facing calendars and only official email addresses should be used to identify members of staff.

- Mobile phones may not be brought into the school by pupils.
- The school allows staff to bring in personal mobile phones and devices for their own use. Staff are permitted to use these during break times as long as there are not children around. Under no circumstances should a member of staff contact a pupil or parent/ carer using their personal device unless authorised to do so by the school.
- The school is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate text messages between any member of the school community is not allowed.
- Users bringing personal devices into the school must ensure there is no inappropriate or illegal content on the device.
- The school provides a safe and secure way of using chat rooms, blogs and other 'social networking technologies' via a Learning Platform or similar system.
- Other 'social networking' facilities may be 'unfiltered' for curriculum purposes. Staff are aware of the procedure they need to follow when requesting access to externally based social networking sites.

**Social Media - Protecting Professional Identity**

All schools and local authorities have a duty of care to provide a safe learning environment for pupils and staff. The school has a policy that sets out clear guidance for staff to manage risk and behaviour online.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school, through limiting access to personal information:

- Training to include: acceptable use, social media risks, checking of settings, data protection
- Clear reporting guidance, including responsibilities, procedures and sanctions

School staff should ensure that:

- No reference should be made in social media to pupils, parents / carers or school staff without the permission of the guardian or person(s) involved.
- They do not engage in online discussion on personal matters relating to members of the school community.
- Personal opinions should not be attributed to the school or local authority.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

The school's use of social media for professional purposes will be checked regularly by the senior risk officer to ensure compliance with the Data Protection.

**Unsuitable or inappropriate activities**

- All monitoring, surveillance or investigative activities are conducted by ICT authorised staff and comply with the Data Protection Act 2018, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000.

The school will take all reasonable precautions to ensure Online safety.
However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device.

- Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:

- Interview/counselling by Class teacher / Child Protection Officer / Online safety Coordinator / Head teacher
- Informing parents or carers
- Removal of Internet or computer access for a period, (which could ultimately prevent access to files held on the system, including examination coursework)
- Referral to LA / Police

- The LA has set out the reporting procedure for Online safety incidents (**Appendix 1**).

- Our Online Safety lead acts as first point of contact for any complaint.
  - Any complaint about staff misuse is referred to the Head teacher.
  - Complaints of cyber-bullying are dealt with in accordance with our Anti-Bullying Policy
  - Complaints related to child protection are dealt with in accordance with school Child Protection procedures.

- There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

**Regular Review**

**Review the online safety policy annually, or more frequently if necessary.**

Consider feedback from stakeholders, emerging risks, and changes in legislation.

**Policy Evaluation**

**Evaluate**

- The internet, information systems, e-mail and all associated devices and technologies that enable access to these play an essential role in our school. These systems and technologies are available to pupils, teaching staff, support staff and other authorised persons to enhance educational and professional activities including teaching, learning, research, administration and management.
- How we communicate reflects both on us as individuals and on the school as a whole. Therefore, whilst respecting personal privacy and autonomy, this policy is here to ensure all members of the school community are fully informed for what is expected in the use of data, e-mail and the internet.
- It is our expectation that all users of ICT in school (hardware and software) do so sensibly, professionally, lawfully and in a manner which is consistent with duties, roles, with respect for others and in accordance with this policy.
- For the safety of the whole school community, the school is able to monitor the use of the internet and e-mail system.
- This policy is for all users of ICT (hardware and software). Any inappropriate use of the school's internet and e-mail systems may lead to disciplinary action.
- It is important that all users of ICT in the school community are familiar with this policy. If any clarification is needed, this should be raised with the Online Safety Co-ordinator or the Head teacher.
- Every pupil, employee or authorised user of ICT in the school's community is required digitally agree with the school's Acceptable Use Agreement annually.

**Sources of support and advice**

UK Safer Internet Centre https://www.saferinternet.org.uk/ - includes a range of activities for children of different ages.
CEOP / Thinkuknow https://www.thinkuknow.co.uk/ - includes a range of home activity packs
National Online Safety https://nationalonlinesafety.com/ - Good guides for parents and staff Parent Info https://parentinfo.org/ - specifically aimed at parents
Internet Matters https://www.internetmatters.org/ - specifically aimed at parents Net Aware https://www.net-aware.org.uk/ - NSPCC's advice on online matters

**Appendix 1**- Guidance procedure for E-Safety Incidents-Staff user incidents

# Guidance reporting procedure for Online Safety incidents involving staff.

In accordance with DGfL Acceptable Use Policies, if you find or suspect that inappropriate or illegal material is being accessed or stored on a PC, laptop, portable device or on the network

Record the account username, station number or approximate time that such material has been accessed and brief description of evidence.

Report incident to Head teacher or designated person in school. *N.B. School may wish to investigate internally and log the incident internally*. If further intervention is required-see below

*Staff should not try to examine files/folders on a machine themselves (particularly if they suspect it contains illegal material) and it should only be examined by those with appropriate forensic skill such as the police.*

Designated person(s) contact DGfL/ managed service provider-01384 814276

DGfL/managed service provider will ask for consent to investigate user account log files (RIPA) and provide information to the designated school contact.

Do the log files contain **illegal** * materials?

Yes

No

*Illegal – prohibited by law or by official or accepted rules

*Inappropriate – not conforming with accepted standards of propriety or taste, undesirable or incorrect behaviour

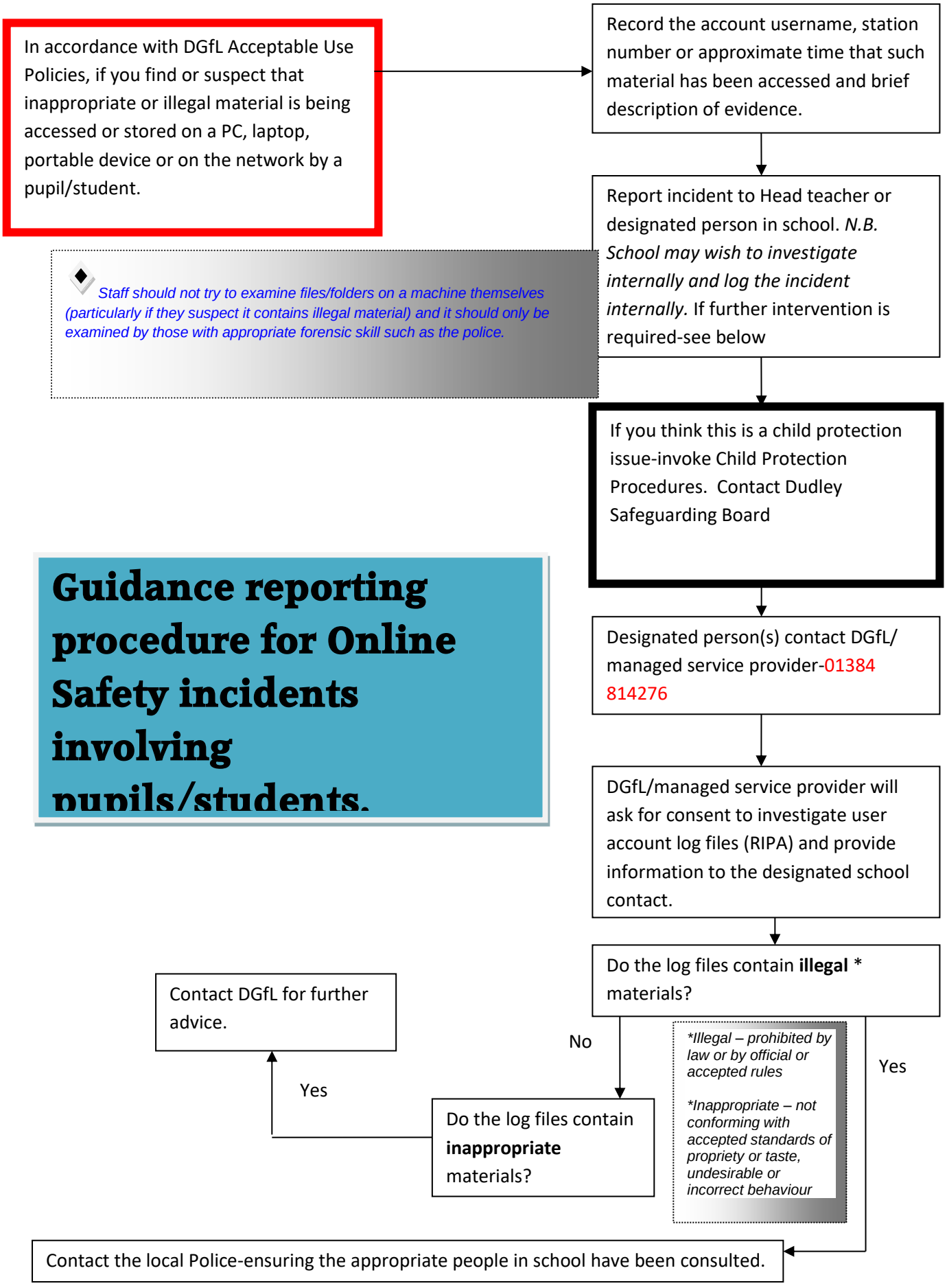
Do the log files contain **inappropriate** materials?

Yes

Contact DGfL for further advice.

Contact the local Police-ensuring the appropriate people in school have been consulted.

**Appendix 1** -Guidance procedure for E-Safety Incidents-Pupil user incidents



**Appendix 2** E-Safety tools available on the DGfL network

| **Online -Safety tool** | **Type** | **Availability** | **Where** | **Details** |
|---|---|---|---|---|
| RM SafetyNet | Web filtering | Provided as part of DGfL | All network connected devices within DGfL | Gives schools the ability to audit, filter and un-filter websites |
| Smoothwall | Monitoring software | Available to all schools who sign an agreement | The *e*-Safe application is securely installed on the school servers, computers, in internet browsers - to monitor a user's online and offline activity, both in school and away from the school network. | Takes a snapshot of a screen when an event is triggered. A range of events are monitored remotely by DBS cleared forensic specialists. Danger risks are phoned through to the Headteacher. Additional, customisable, non-danger-risk reports are provided to the school. |
| CC4 AUP | Awareness raising | Part of CC4- needs to be enabled | All CC4 stations (computers and laptops) at log in | When enabled through the management console, users are given an acceptable use policy at log in |
| Email | Filtering and list control | Provided as part of DGfL | Office 365 | Allows schools to restrict where email is sent from/to |
| RM Password Plus | Safe practice | Provided as part of DGfL3 | All CC4 stations | A password management tool that enforces password rules of complexity and length for different users |

**Appendix 3** Amblecote Primary School Staff Acceptable Use policy

Rules for Responsible Internet use

This policy applies to all adult users of the schools' systems. We trust you to use the ICT facilities sensibly, professionally, lawfully, consistent with your duties, with respect for your colleagues and in accordance with this Policy.

It is important that you read this policy carefully. If there is anything that you do not understand, please discuss it with the Head Teacher or your line manager. Once you have read and understood this policy thoroughly, you should sign this document, retain a copy for your own records and return the original to the Head Teacher

Any inappropriate use of the school's internet & e-mail systems whether under this policy or otherwise may lead to disciplinary action being taken against you under the appropriate disciplinary procedures which may include summary dismissal. Electronic information can be produced in court in the same way as oral or written statements.

Research Machines (RM) has a contractual obligation to monitor the use of the internet and e-mail services provided as part of DGfL, in line with the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000. Traffic data and usage information may be recorded and may be used in disciplinary procedures if necessary. RM, Dudley MBC and the school reserve the right to disclose any information they deem necessary to satisfy any applicable law, regulation, legal process or governmental request. If there is any evidence that this particular policy is being abused by individuals, we reserve the right to withdraw from employees the facility to view, send and receive electronic communications or to access the internet.

All information relating to our pupils, parents and staff is personal. You must treat all school information with the utmost care whether held on paper or electronically.

Official school systems must be used at all times.

Use of the Internet and Intranet

When entering an internet site, always read and comply with the terms and conditions governing its use. Be aware at all times that when visiting an internet site, the unique address for the computer you are using (the IP address) can be logged by the site you visit, thus identifying your school. For your information, the following activities are criminal offences under the Computer Misuse Act 1990:

· Unauthorised access to computer material i.e. hacking;

· Unauthorised modification of computer material; and

· Unauthorised access with intent to commit/facilitate the commission of further offences.

In line with this policy, the following statements apply:-

· If you download any image, text or material check if it is copyright protected. If it is then follow the school procedure for using copyright material.

· Do not download any image, text or material which is inappropriate or likely to cause offence. If this happens accidentally report it to a senior member of staff.

· If you want to download any software, first seek permission from the Head Teacher and/or member of staff responsible /RM. They should check that the source is safe and appropriately licensed.

· If you are involved in creating, amending or deleting web pages or content on the web site, such actions should be consistent with your responsibilities and be in the best interests of the School.

· You should not :

o Introduce packet-sniffing software (i.e. software which is used to intercept data on a network) or password detecting software;

o Seek to gain access to restricted areas of the network;

o Knowingly seek to access data which you are not authorised to view;

o Introduce any form of computer viruses;

o Carry out other hacking activities.

o Access online gaming or gambling

o Access online gaming

Electronic Mail

Care must be taken when using e-mail as a means of communication as all expressions of fact, intention or opinion may implicate you and/or the school.

Internet and e-mail access is intended to be used for school business or professional development, any personal use is subject to the same terms and conditions and should be with the agreement of your head teacher. Your privacy and autonomy in your business communications will be respected. However, in certain circumstances it may be necessary to access and record your communications for the School's business purposes which include the following:

1. providing evidence of business transactions;
2. making sure the School's business procedures are adhered to;
3. training and monitoring standards of service;
4. preventing or detecting unauthorised use of the communications systems or criminal activities;
5. maintaining the effective operation of communication systems.

In line with this policy the following statements apply:-

· You should agree with recipients that the use of e-mail is an acceptable form of communication. If the material is confidential, privileged, or sensitive you should be aware that un-encrypted e-mail is not secure.

· Do not send sensitive personal data via email unless you are using a secure site or portal. It is good practice to indicate that the email is 'Confidential' in the subject line.

· Copies of emails with any attachments sent to or received from parents should be saved in a suitable secure directory.

· Do not impersonate any other person when using e-mail or amend any messages received.

· Sending defamatory, sexist or racist jokes or other unsuitable material via the internet or email system is grounds for an action for defamation, harassment or incitement to racial hatred in the same way as making such comments verbally or in writing.

· It is good practice to re-read e-mail before sending them as external e-mail cannot be retrieved once they have been sent.

· If the email is personal, it is good practice to use the word 'personal' in the subject header and the footer text should indicate if it is a personal email the school does not accept responsibility for any agreement the user may be entering into.

· Internet and e-mail access is intended to be used for school business or professional development, any personal use is subject to the same terms and conditions and should be with the agreement of your headteacher.

· All aspects of communication are protected by intellectual property rights which might be infringed by copying. Downloading, copying, possessing and distributing material from the internet may be an infringement of copyright or other intellectual property rights.

Social networking

The use of social networking sites for business and personal use is increasing. Access to social networking sites is blocked on the school systems, however a school can manage access by un-filtering specific sites, internet usage is still monitored.

School staff may need to request access to social networking sites for a number of reasons including:

· Advertising the school or managing an 'official' school presence,

· For monitoring and viewing activities on other sites

· For communication with specific groups of adult users e.g. a parent group.

Social networking applications include but are not limited to:

· Blogs

· Any online discussion forums, including professional forums

· Collaborative spaces such as Wikipedia

· Media sharing services e.g. YouTube, Flickr

· ‘Microblogging’ applications e.g. Twitter

When using school approved social networking sites the following statements apply:-

· School equipment should not be used for any personal social networking use

· Staff must not accept friendships from underage pupils. The legal age for students to register with a social networking site is usually 13 years; be aware that some users may be 13 or younger but have indicated they are older.

· It is important to ensure that members of the public and other users know when a social networking application is being used for official school business. Staff must use only theirname@amblecote. dudley.sch.uk email address or other school approved email mechanism and ensure all contributions are professional and uphold the reputation of the school.

· Social networking applications should not be used to publish any content which may result in actions for defamation, discrimination, breaches of copyright, data protection or other claims for damages. This includes but is not limited to material of an illegal, sexual or offensive nature that may bring the school into disrepute.

· Postings should not be critical or abusive towards the school, staff, pupils or parents or used to place a pupil, student or vulnerable adult at risk of harm

· The social networking site should not be used for the promotion of personal financial interests, commercial ventures or personal campaigns, or in an abusive or hateful way

· Ensure that the appropriate privacy levels are set. Consider the privacy and safety settings available across all aspects of the service – including photos, blog entries and image galleries. Failing to set appropriate privacy levels could result in messages which are defamatory, libellous or obscene appearing on your profile before you have chance to remove them.

· It should not breach the schools Information Security policy

Data protection

The processing of personal data is governed by the Data Protection Act 2018, Schools are defined in law as separate legal entities for the purposes of complying with the Data Protection Act. Therefore, it is the responsibility of the school, and not the Local Authority, to ensure that compliance is achieved.

As an employee, you should exercise due care when collecting, processing or disclosing any personal data and only process personal data on behalf of the school. The main advantage of the internet and e-mail is that they provide routes to access and disseminate information.

Through your work personal data will come into your knowledge, possession or control. In relation to such personal data whether you are working at the School’s premises or working remotely you must: -

· Keep the data private and confidential and you must not disclose information to any other person unless authorised to do so. If in doubt, ask your Head Teacher or line manager;

· Familiarise yourself with the provisions of the Data Protection Act 2018 and comply with its provisions;

· Familiarise yourself with all appropriate school policies and procedures;

· Familiarise yourself with the three levels of data security levels 0 to 3

· Not make personal or other inappropriate remarks about staff, pupils, parents or colleagues on manual files or computer records. The individuals have the right to see all information the school holds on them subject to any exemptions that may apply.

· DO NOT use removable media (dig sticks, portable hard drives, laptops etc.) to transport confidential/secure data (refer to three level criteria).

· Use cloud technology to access confidential/secure data i.e., Portal, CC4 Anywhere, Office 365 SkyDrive.

If you make or encourage another person to make an unauthorised disclosure knowingly or recklessly you may be held criminally liable.

Tablets / iPads Acceptable Use Policy - Staff

The policies, procedures and information within this document apply to the tablet devices (iPads) and are in addition to the current ICT Acceptable Use Policy.

Users Responsibilities

· Users must use protective covers/cases for their iPad.

· The iPad screen is made of glass and therefore is subject to cracking and breaking if misused: Never drop nor place heavy objects (books, laptops, etc.) on top of the iPad.

· Only a soft cloth or approved laptop screen cleaning solution is to be used to clean the iPad screen.

· Do not subject the iPad to extreme heat or cold.

· It is a user's responsibility to keep their iPad safe and secure. Ensure the mobile device is secured or locked away when not in use.

· The whereabouts of your iPad should be known at all times.

· If the iPad is lost, stolen, or damaged, the school Office must be notified immediately. Outside of the school premises, the iPads are not covered by the school's insurance policy. Any damage, loss of or theft will be the responsibility of the staff member. The actual cost of replacement will be determined by Apple/RM but will not exceed the retail value of like-for-like replacement.

· The iPad is subject to routine monitoring. Users in breach of the Acceptable Use Policy may be subject to but not limited to, disciplinary action, confiscation, removal of content or referral to external agencies in the event of illegal activity.

· iPads are intended for use at school each day and staff are responsible for keeping their iPad's battery charged.

· iPads are intended for academic use at school.

· Users must use good judgment when using the camera. The user agrees that the camera will not be used to take inappropriate photographs or videos. Please be mindful of our safeguarding and data protection requirements when using images of other people.

· Users should be aware of and abide by the guidelines set out by the School digital devices / ICT policy.

· The School reserves the right to confiscate and search any Mobile Device to ensure compliance with this Responsible Use Policy.

· Jailbreaking is the process which removes any limitations placed on the Mobile Device by Apple. Jailbreaking results in a less secure device and is strictly prohibited, it also negates any warranties and insurances taken out against the device.

· The iPad remains the property of Amblecote Primary School.

· Please complete a Staff Guardianship loan form if the device/iPad is required to be used out of the school premises.

I have read through and fully understand the terms of the policy. I also understand that the school may amend this policy from time to time and that I will be issued with an amended copy.

**Appendix 4**

## Pupil Acceptable Use Policy Agreement

This is how we stay safe when we use computers:

### Foundation Stage and Key Stage 1

- I will ask a teacher or suitable adult if I want to use the computers / tablets.
- I will only use activities that a teacher or suitable adult has told or allowed me to use.
- I will take care of the computer and other equipment.
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong.
- I will tell a teacher or suitable adult if I see something that upsets me on the screen.
- I know that if I break the rules I might not be allowed to use a computer / tablet.

### Key Stage 2. All the above and the following

- I will not share any of my passwords with anyone or use another person's password. If I find out someone else's password, I will tell that person and a member of the school staff so they can change it.
- I will be respectful in how I talk to and work with others online and never write or participate in online bullying. If anyone sends me a message, I do not like or feel uncomfortable about I will show it to my teacher or parent.
- I will report any unpleasant material or messages sent to me. I understand my report would be confidential and would help protect other pupils and myself.
- I will not download any programmes or games on to the school computers, netbooks or laptops unless I have permission to do so.
- I will always check with a responsible adult before I share or publish images of myself, my friends or other people onto the internet.
- When using sites on the internet, I will not give my name, home address, telephone/mobile number, pretend to be someone else or arrange to meet someone I do not know, unless my parent, carer or teacher has given permission.
- ***I know anything I do on the computer may be seen by someone else.***

***I am aware of the CEOP report button and know when to use it.***