# Ravenswood School
# Online Safety Policy

**Purpose**
This policy applies to all members of the school community (including staff, students, governors, volunteers, parents / carers, visitors and community users) both in school and out of school. (Detailed roles and responsibilities can be found in Appendix C). It is a statement of the aims, principles, strategies and procedures for online safety throughout the school. The policy provides the framework to nurture a safe digital community.

The Online Safety Policy should be read in conjunction with our Data Protection and Information Sharing Policy, Social Media and Networking Policy, Safeguarding Policy and Whistleblowing Policy. There is other legislation and guidance that should also be considered when adhering to this policy (see Appendix N).

**What is Online Safety?**
While cybersecurity protects devices and networks from harm by third parties, Online Safety protects the people using them from harm by the devices and networks (and therefore third parties) through awareness, education, information and technology.

It is what we call the appropriate approach to personal safety when using digital technologies.

Online Safety is being aware of the nature of the possible threats that you could encounter whilst engaging in activity through the Internet, these could be security threats, protecting and managing your personal data, online reputation management, and avoiding harmful or illegal content.

The DfE Keeping Children Safe in Education guidance suggests that:

> *The breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk:*
>
> ***content**: being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.*
>
> ***contact**: being subjected to harmful online interaction with other users; for example: 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**: online behaviour that increases the likelihood of, or causes, harm; for example, 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*

The internet is accessible from computers, laptops, tablets, smartphones, games consoles and other devices like smart watches and connected TVs. Other communication technologies such as texting and phone calls are also covered by the term 'Online Safety'.

**Why provide Internet Access?**
The internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality internet access as part of their learning experience. The internet is part of the statutory curriculum and an entitlement for pupils as part of their learning experience. It is used in this school to raise educational standards, promote pupil achievement and as a necessary tool for staff to support their professional work. The internet is also essential for the school's management information, business administration and child protection systems.

## School Policy on the use of ICT

**Internet**

- Pupils will be taught what internet use is acceptable and what is not. They will be given clear objectives for internet use.
- Staff should guide pupils in online activities that will support the learning outcomes planned for the pupils' age and maturity.
- Internet access will be planned to enrich and extend learning activities.
- Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils are required to return a signed copy of the ICT Acceptable Usage Agreement for Pupils every year which must be countersigned by their parent or carer (see Appendix E) - now part of the Home-School Agreement.
- All staff and visitors to school must read and sign the ICT Acceptable Usage Agreement for Staff, Governors, Visitors and Community Users before using any school ICT resources (see Appendix D).
- Pupils will be encouraged to tell a teacher immediately if they encounter any material that makes them feel uncomfortable.
- Pupils will be taught to question information before accepting it as true.
- School internet access will be differentially filtered appropriate to the needs of staff to carry out their roles effectively and the ability of pupils to use it within school rules.
- The school will ensure that use of internet derived materials by staff and pupils complies with copyright law.

**Accounts and Messaging**

- Staff and pupils may only use official school accounts on school devices. Personal accounts are not to be used.
- All messages sent must be professional in tone and content.
- The sending of abusive or inappropriate text messages is forbidden.
- Personal accounts must not be used for communication between staff and students or parent/carers.
- If personal information is to be emailed to an external address it is essential that it's sent securely, through our school Egress Protect service. Personal or confidential information sent to an external recipient in a standard email might constitute a data breach.
- Emails containing personal or confidential information must be identified by the sender in the email subject with the word PROTECTED.
- Pupils must have adult supervision whilst using messaging services.
- Pupils must immediately tell a teacher if they receive an offensive message.

- Pupils must not reveal personal details of themselves or others in message communication (such as address or telephone number). Pupils must not arrange to meet anyone without specific permission.
- Messages sent to an external organisation should be written carefully and authorised by a member of staff before sending. Pupils are blocked from emailing externally so a member of staff would need to forward the email.
- Pupils will be made aware that the writer of a message (or the author of a web page) may not be the person claimed.

**Social Networking**
**Workers at the school shall:**

- Act in accordance with our Social Media and Networking Policy.
- Act in accordance with our Whistleblowing Policy.

**Chatrooms and Instant Messaging**

- The use of these facilities is permitted only through monitored, official school systems like Office 365.

**Video Communications**

- Visitors / contributors may be invited to join (supervised) lessons through a video call using Teams or Zoom in accordance with the Visitor to School Policy.
- Pupils will not be allowed unsupervised access to video communications

**Digital communication should take place using <u>only</u> official monitored school systems and must be professional in tone and content. Between staff and students; official Office 365 and Seesaw. Between staff and parents/carers; Seesaw, ParentPay, official Office 365. Between school and the wider community; school website, official school social media accounts, official Office 365.** Specific permission from the Headteacher should be sought for any exceptions e.g. setting up a blog for students, as required by the curriculum.

**Mobiles, cameras and portable digital devices**

**Pupils:**

- Mobile phones, smart watches, cameras, tablets, portable electronic games and media players brought into school by pupils must be handed-in at the school office unless the Headteacher has given permission e.g. for communication aids.
- If a pupil is found to be in possession of one of these electronic devices our behaviour Management Policy gives details on how a search for the item can be made.

**Staff:**

- Use of personal devices in school such as computers, tablets, watches with smartphone notifications and any device with the functionality to take pictures, videos or make sound recordings, is not permitted. Exceptions to this rule are personal mobile phones or any device with specific written permission from the Headteacher.
- Staff may only use personal mobile phones in designated areas. These areas are the Admin Team offices, the staff room and the car park.
- Use of personal mobile phones in school must be within the ICT Acceptable Usage Agreement.
- Staff must not keep or use personal mobile phones in view of children (e.g. if there are pupils in the staff room or offices).
- Staff must not use personal devices to take any images, video or sound recordings of pupils.
- Staff must not take inappropriate images.

- Staff are allowed to take digital photographs and video images of pupils on school devices to support educational aims but follow guidance in the ICT Acceptable Usage Agreement for Staff, Governors, Visitors and Community Users concerning the taking, sharing, distribution and publication of those images. These must not be taken in non-designated areas (including toilets and changing rooms).
- Text messaging must not be used for communication between staff and pupils unless used for the educational benefit of pupils with all parties using school-issued devices and specific written permission has been obtained from the Headteacher.
- Teachers who are issued with class iPads must sign the appropriate agreement (see Appendix F)
- Staff who are issued with iPads must sign the appropriate agreement (see Appendix G)
- Staff who are issued with laptops must sign the appropriate agreement (see Appendix H)

**Memory Sticks and other portable storage**

This includes portable USB flash drives and portable hard disk drives.

- The Information Commissioner's Office has the power to impose hefty fines on schools and individuals who lose personal data or allow it to escape into the public domain. The loss of an unencrypted memory stick containing the names of pupils would count. The school has therefore taken the decision to ban the use of memory sticks and portable hard disk drives in school (other than those used for backup purposes by the Network Manager in accordance with school policies). There will be sanctions for any breach of this policy.
- Memory sticks or portable hard disk drives may be used in exceptional circumstances with specific written permission from the Headteacher.
- Media card readers may be used with school computers to retrieve photos and video from school-owned camera cards (e.g. SD cards).
- The school's Data Protection and Information Sharing Policy applies.

**Optical Discs**

School data in any form (documents, pictures, videos etc) will not be burned to optical disc except:

- when archiving data to be stored securely at school
- when submitting pupil work to examining bodies
- with specific written permission from the Headteacher

**School Website**

- The point of contact on the website will be the school address, email and telephone number. Staff or pupils' personal information will not be published.
- Website photographs that include pupils will be selected carefully and will only be published with parental permission.
- Pupils' full names will not be used anywhere on the website.
- The Headteacher will delegate editorial responsibility to the Network Manager to ensure that content is accurate and quality of presentation is maintained.

**Cyberbullying**

Cyberbullying is the use of the internet and related technologies to harm other people, in a deliberate, repeated, and hostile manner. When children are the target of bullying via mobile phones, gaming or the internet, they can often feel very alone and, a once safe and enjoyable environment or activity can become threatening, harmful and a source of anxiety.

- Pupils will be taught about the effects of cyberbullying
- Pupils will be encouraged to keep any evidence of cyberbullying

- Pupils will be made aware that the police will be able to trace the originator of any messages
- Cyberbullying (along with all forms of bullying) will not be tolerated in school. All incidents reported will be recorded and investigated.

**Filtering**
The school Filtering Policy applies (see Appendix K)

**Monitoring**
The Network Manager will regularly check:
- SWGfL logs of internet activity
- Impero logs of the usage of keywords and phrases

Where a need has been identified, the Network Manager and the Headteacher will check, for pupils or staff:
- Files stored on school computers
- School email
- Impero logs of internet activity
- Use of social networking websites

Illegal misuse will be dealt with in accordance with the procedure detailed in Appendix B.

**School ICT and Data Security**
- The school Data Protection and Information Sharing Policy applies.
- The school Password Security (Appendix J), Filtering (Appendix K) and the ICT Service Continuity Management (Appendix L) requirements apply.
- Users must not share their user account details and must not leave their computers unlocked and accessible to others.
- Official remote communication channels into school systems will be encrypted.
- Personal data sent over the internet will be encrypted.
- Unapproved system utilities and executable files are not permitted on school equipment.
- Remote access to school Office 365 may be made from personally-owned devices, however, it is essential that usage is kept within the rules set out in the ICT Acceptable Usage Agreement (Appendix D).
- The access or storage of personal or confidential data on any device not owned by the school is not permitted. If a school attachment or file containing such data has been opened locally on a device the user must make appropriate arrangements for the file to be securely deleted to prevent information being retained on the device.
- Suspected data breaches must be immediately logged in GDPRiS or, if that is not possible, reported to the Headteacher, as an Information Security Incident.
- Virus protection updates and system updates for PCs will be regularly installed.
- School ICT system security will be reviewed regularly.

**Policy Enforcement**
The Online Safety Co-ordinator will ensure that the Online Safety Policy is implemented and compliance with the policy monitored. Appendix A shows which activities are deemed 'Acceptable' or 'Unacceptable'.

Any unacceptable or illegal activities will result in disciplinary procedures being instigated.

**Pupils:**
- All pupils and their parents/carers must sign the ICT Acceptable Usage Agreement for Pupils every year (it forms part of the Home-School Agreement).

- The ICT Acceptable Usage Agreement for Pupils will often be referred to in lessons.
- Online Safety rules will be posted in all rooms where computers are used and will be discussed with pupils at the start of each academic year.
- Pupils will be informed that internet use will be monitored and sanctions will be imposed if the facility is abused.
- Any breaches of the ICT Acceptable Usage Agreement for Pupils will be referred directly to the Online Safety Co-ordinator.
- The school will keep a record of all pupils who have been denied internet access and the reason and length of time it was denied.
- Pupils will be informed that network and internet use will be monitored.
- Pupils' work will only be published online with the permission of the pupil and parent/carer.
- There may be occasions when discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

**Staff:**

- All staff must read and sign the ICT Acceptable Usage Agreement for Staff, Governors, Visitors and Community Users before using school ICT resources and annually thereafter.
- The school will keep a record of all staff who have been denied internet access and the reason and length of time it was denied.
- All staff including teachers, supply staff and support staff, will be told how to access this Online Safety Policy, and its importance will be explained.
- Staff will be made aware that professional conduct is essential when using school ICT and that internet use will be monitored and can be traced to the individual user.
- Any breaches of the ICT Acceptable Usage Agreement for Staff will be referred directly to the Headteacher.
- The school will audit ICT provision to establish if the Online Safety Policy is adequate and its implementation effective.
- Responsibility for handling incidents of internet misuse will lie with the Family Support Advisor who will liaise with the Online Safety Co-ordinator.

**Complaints**

- Any complaint about staff misuse of ICT must be referred to the Headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school safeguarding procedures.
- Pupils and parents will be informed of the complaints procedure via the school website.
- Parents and pupils will need to work in partnership with staff to resolve issues.

**Parental Support**

- Parents' attention will be drawn to the school Online Safety Policy in newsletters, the school website, during online safety events and during the annual Safer Internet Week.
- Parents will be asked to read through the ICT Acceptable Usage Agreement for Pupils with their child and co-sign the agreement (it forms part of the Home-School Agreement).
- Internet issues will be handled sensitively to inform parents without undue alarm.
- A partnership approach with parents will be encouraged. This could include demonstrations, practical sessions and suggestions for safe internet use at home.

**Education & Training: Staff and Governors**
There is a planned programme of online safety training for all staff and governors to ensure they understand their responsibilities, as detailed in this, and the ICT Acceptable Usage Agreement for Staff, Governors, Visitors and Community Users.

- All new staff receive e-safety training as part of their induction programme
- The Online Safety Co-ordinator receives regular updates through attendance of online safety conferences.
- This Online Safety Policy and its updates are shared and discussed in staff meetings. Updates are provided to all staff.
- The Online Safety Co-ordinator provides advice/guidance and training as required and seeks LA advice on issues where required.

**Education: Pupils**
Whilst regulation and technical solutions are very important, their use must be balanced with educating learners to take a responsible approach. The education of students in online safety is therefore an essential part of the school's online safety provision. Pupils need the help and support of the school to recognise and avoid online safety risks and build their resilience.

- There is a planned online safety scheme of work and timetabled computing lessons.
- Key online safety messages are reinforced annually through assemblies, time to talk, across all subject areas and annually during Safer Internet Week.
- Pupils are helped to understand and act in accordance with the ICT Acceptable Usage Agreement for Pupils.
- Pupils are taught to acknowledge the sources of information they use and to respect copyright when using material accessed on the internet.
- The ICT Acceptable Usage Agreement for Pupils is displayed in all rooms where ICT is used.
- Online safety is a focus in all relevant areas of the curriculum.
- In lessons where internet use is pre-planned, pupils are guided to sites checked as suitable for their use and processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, e.g. using search engines, staff are vigilant in monitoring the content of the websites the young people visit and encourage pupils to use specific search terms to reduce the likelihood of coming across unsuitable material.
- Students are taught to be critically aware of the materials / content they access online and be guided to validate the accuracy of information.
- When using digital images, pupils are taught about the risks associated with the taking, use, sharing, publication and distribution of images including on social networking sites.
- Staff act as good role models in their own use of ICT.
- Staff are familiar with and ensure that pupils act in accordance with the ICT Acceptable Usage Agreement for Pupils.

**Education: Parents/Carers**
Parents and carers may have only a limited understanding of online safety issues and may be unaware of risks and what to do about them. However, they have a critical role to play in supporting their children with managing online safety risks at home, reinforcing key messages about online safety and regulating their home experiences. The school supports parents to do this by promoting online safety through the school website, newsletter, leaflets and online safety sessions.

**Risk**
The school will take all reasonable steps to mitigate the risks identified above and ensure that

users create and access only appropriate 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 school computer. An Online Safety Co-ordinator has been appointed to oversee internet dangers, risk assessment and matters arising from internet use. However, neither the school nor North Somerset Council can accept liability for the material accessed, or any consequences of internet access.

**Development, monitoring and review of the policy**
This Online Safety Policy has been developed, and will be monitored, by our school Online Safety Committee which comprises:

- Headteacher
- Online Safety Co-ordinator
- Computing Subject Leader
- Curriculum Lead
- E-Safety Governor

The committee meets regularly and uses the 360safe.org.uk online safety self-review tool to monitor 21 aspects of online safety to develop our provision and feed back into this policy. Terms of reference of the committee can be found in Appendix M.

Consultation with the whole school community has taken place through staff meetings, Student Council meetings, Governors' meetings, Safer Internet Week, the school website and the school newsletter.

The school will monitor the impact of the policy using:
- Logs of reported incidents
- Logs of internet activity
- Logs of computer use through key words
- Other internal monitoring data
- Surveys of students, parents/carers and staff (including non-teaching staff)

The policy will be reviewed immediately where monitoring data shows a need. The policy will also be reviewed annually.

**History of Document**

| Issue No. | Author | Date Reviewed | Approved by Governors on: | Comments |
|---|---|---|---|---|
| 1. | A Pester | 08/2012 | FGB 05/09/2012 | |
| 2. | P Clark | 11/2013 | Business Committee 28/11/2013 | No changes required. |
| 3. | A Pester | 01/2015 | 22/01/2015 Business Committee | Simplification and clarification throughout policy and appendices. Addition of 'Staff Proxy' section in Appendix K. |
| 4. | A. Pester | 01/2016 | Pupil Committee 11/05/2016 | |
| 5. | A Pester | 01/2018 | 19/01/2018 | |
| 6. | A Pester | 01/2019 | 23/01/2019 | |
| 7. | A Pester | 01/2020 | 22/01/2020 | General updates throughout.<br>Addition of smart watches as devices not permitted in school.<br>Addition of rules around accessing school Office 365 from personal devices. Removal of Remote Access Agreement (previously Appendix F) and incorporation of clauses into ICT Acceptable Usage Agreement (Appendix D). |
| 8. | A Pester | 01/2021 | 20/01/2021 | Update of iPad and laptop agreements (Appendices F, G and H). Addition of pupil laptop agreement (Appendix I). |
| 9. | A. Pester | 01/2022 | 26/01/2022 | No updates |
| 10. | K Barnes | 01/2023 | 18/01/2023 | Minor updates for clarity |
| 11. | A Pester | 01/2024 | 17/01/2024 | General updates throughout. Removal of Appendix M: 'Use of Internet and Social Networking Sites', as this is covered in our Social Media and Networking Policy. Addition of new Appendix M: 'Terms of Reference of the Online Safety Committee'. Change of rules in Appendix D around the use of devices not owned by the school. |

## Appendix A

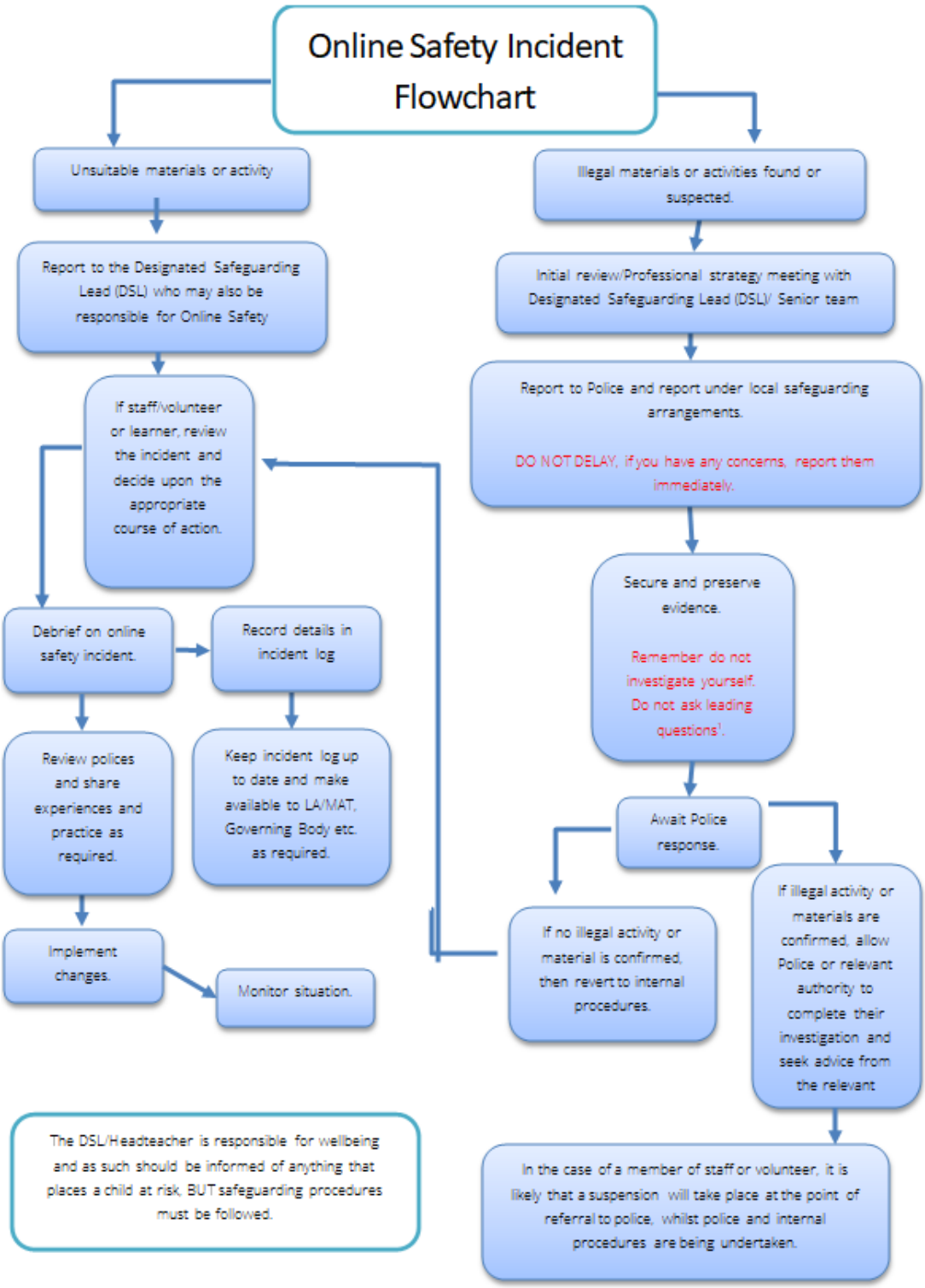
**Unsuitable / inappropriate activities**
Activities will be treated in accordance with the following table. Any unacceptable or illegal activities will result in disciplinary procedures being instigated.

| User Actions | | Acceptable | Acceptable at certain times | Acceptable with specific written permission from the Headteacher | Will result in disciplinary action | |
|---|---|---|---|---|---|---|
| | | | | | Unacceptable | Unacceptable and illegal |
| **Any connection with:** | child sexual abuse images | | | | | ■ |
| | promotion or conduct of illegal acts, e.g. under child protection, obscenity, computer misuse and fraud legislation | | | | | ■ |
| | adult material that potentially breaches the Obscene Publications Act in the UK | | | | | ■ |
| | criminally racist material in UK | | | | | ■ |
| | promotion of any kind of discrimination | | | | ■ | |
| | promotion of racial or religious hatred | | | | ■ | |
| | threatening behaviour, including promotion of physical violence or mental harm | | | | ■ | |
| | pornography | | | | ■ | |
| | any other behaviour which may be offensive to colleagues, breaches the integrity of the ethos of the school or brings the school into disrepute | | | | ■ | |
| Using school systems to run a private business | | | | | ■ | |
| Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by SWGfL and / or the school | | | | | ■ | |
| Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions | | | | | ■ | |
| Revealing or publicising confidential or proprietary information (e.g. financial / personal, databases, computer / network access codes and passwords) | | | | | ■ | |
| Creating or propagating computer viruses or other harmful files | | | | | ■ | |
| Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet | | | | | ■ | |
| Online gaming (educational) | | | ■ | | | |
| Online gaming (non-educational) | | | ■ | | | |
| Online gambling | | | | | ■ | |
| Online shopping / commerce (Staff) | | | ■ | | | |
| Online shopping / commerce (Pupils) | | | | | ■ | |
| Use of school email system to send personal emails that comply with the ICT AUA for Staff and Community Users | | | ■ | | | |
| Installing software on school PCs without the permission of the Network Manager | | | | | ■ | |
| Use of public social networking sites e.g. Bebo, Facebook, X | | | | ■ | | |

## Appendix B

### Responding to incidents of misuse

We expect all members of the school community to be responsible users of ICT who understand and follow this policy. However, there may be times when infringements of the policy take place. In these cases the SWGfL flow chart below is consulted and followed.




Illegal activity would include those activities listed in Appendix A.

# Appendix C

**Roles and Responsibilities**
These are detailed in the following table:

| Role | Responsibility |
|---|---|
| **Headteacher and Senior Leaders** | • The Headteacher / Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and to support those colleagues who take on important monitoring roles. |
| **Headteacher** | • Ensure the safety (including online safety) of members of the school community, though the day-to-day responsibility for online safety will be delegated to the Online Safety Co-ordinator.<br>• Ensure that all staff receive suitable CPD to carry out their online safety roles and sufficient resource is allocated.<br>• Follow correct procedure in the event of a serious online safety allegation being made against a member of staff.<br>• Inform the local authority about any serious online safety issues.<br>• Ensure that policies and procedures referred to within this policy are implemented. |
| **Senior Leadership Team** | • The Senior Leadership Team will receive regular monitoring reports from the Online Safety Co-ordinator. |
| **Online Safety Co-ordinator** | • Lead the Online Safety Committee in dealing with day-to-day online safety issues.<br>• Take a lead role in establishing / reviewing online safety policies / documents.<br>• Ensure all staff are aware of the procedures outlined in policies.<br>• Ensure that this Online Safety Policy is implemented and compliance with the policy monitored.<br>• Provide and/or broker training and advice for staff.<br>• Maintain online safety CPD and liaise with South West Grid for Learning and North Somerset Council online safety staff and school technical staff.<br>• Deal with and log online safety incidents.<br>• Meet with the Online Safety Committee regularly to discuss incidents and review the online safety log.<br>• Report regularly to the Senior Leadership Team. |
| **Online Safety Committee** | • See Appendix M: Online Safety Group Terms of Reference. |
| **Designated Safeguarding Officer** | DSOs should be trained in online safety issues and be aware of the potential for serious child protection issues to arise from:<br>• sharing of personal data<br>• access to illegal / inappropriate materials<br>• inappropriate online contact with adults / strangers<br>• potential or actual incidents of grooming<br>• cyber-bullying |

| | |
|---|---|
| **Network Manager** | • Ensure the school's ICT infrastructure is secure and is not open to misuse or malicious attack.<br>• Ensure the school meets the online safety technical requirements outlined in the SWGfL Security Policy and gov.uk guidance: 'Meeting digital and technology standards in schools and colleges'.<br>• Ensure that the school's Password Security requirements are fully implemented.<br>• Ensure that use of school ICT systems is regularly monitored and any misuse is dealt with in accordance with school policies.<br>• Manage the school's filtering in accordance with Appendix K: Ravenswood School Filtering.<br>• Report regularly to the Online Safety Committee with monitoring and filtering logs as detailed in Appendix K.<br>• Report online safety concerns to the Online Safety Co-ordinator.<br>• Ensure that SWGfL is informed of issues relating to the filtering they apply<br>• Carry out online safety training for new staff as part of the induction process.<br>• Dispose of ICT hardware in accordance with the Data Protection and Information Sharing Policy.<br>• Delete user accounts and data for staff and pupil leavers in accordance with the Data Protection and Information Sharing Policy and maintain a log of the deleted data.<br>• Record details of the access rights held by groups of users and present this to the Online Safety Committee for annual review.<br>• Ensure that the Network Manager maintains his/her CPD with regard to online safety technical information in order to effectively carry out his/her online safety role and to inform and update others as relevant.<br>• Make regular backups of school systems and handle backup media in accordance with the Data Protection and Information Sharing Policy.<br>• Maintain an inventory of and audit all school ICT equipment such as desktop and laptop computers and all portable devices e.g. ipads and cameras.<br>• Act in accordance with the ICT Service Continuity Management requirements (Appendix L) to develop an ICT Service Continuity Recovery Plan. |
| **Curriculum Leaders** | • Ensure that online safety is embedded throughout the curriculum and other school activities. |
| **Teaching and Support Staff** | • Read, understand, sign and comply with the ICT Acceptable Usage Agreement for Staff, Governors, Visitors and Community Users.<br>• Act in accordance with the Online Safety Policy.<br>• Lock or log-off computers after use and keep passwords secret.<br>• Report any suspected misuse or problem.<br>• Participate in any training and awareness raising sessions<br>• Monitor ICT activity in lessons and extra-curricular and extended school activities.<br>• In line with their capability, ensure that pupils understand and follow the Pupil ICT AUP.<br>• Ensure that pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.<br>• Ensure they are aware of online safety issues related to the use of mobile phones, cameras and hand-held devices and that they act on school policies in relation to the use of these devices. |

| | |
|---|---|
| | • Ensure that in lessons, where internet use is pre-planned, pupils are guided to sites checked as suitable for their use. Follow the processes in place for dealing with any unsuitable material that is found in internet searches. |
| **Students / pupils** | • Participate in online safety activities, follow the ICT Acceptable Usage Agreement and report any suspected misuse.<br>• Understand that the Pupil ICT AUA covers actions out of school that are related to their membership of the school. |
| **Governors** | • Approve and review the effectiveness of the Online Safety Policy and acceptable usage policies.<br>• The Online Safety Governor should attend Online Safety Committee meetings, ensure that regular monitoring of online safety incident logs, filtering logs and monitoring logs takes place and report to Governors at Full Governing Body meetings. |
| **Parents and Carers** | • Endorse (by signature) the ICT Acceptable Usage Agreement for Pupils.<br>• Ensure that their child / children follow acceptable use rules at home.<br>• Discuss online safety issues with their child / children and monitor their home use of ICT systems (including mobile phones and games devices) and the internet.<br>• Access school ICT systems in accordance with the relevant school ICT Acceptable Usage Agreement.<br>• Keep up to date with issues through school updates and attendance at events. |
| **Community Users** | • Sign and follow the ICT Acceptable Usage Agreement for Staff, Governors, Visitors and Community Users before being provided with access to school systems. |

## Appendix D

## ICT Acceptable Usage Agreement for Staff, Governors, Visitors and Community Users

All ICT systems within school are used to help students with their learning and for staff to fulfil duties including teaching, research, administration and management. This Agreement has been drawn-up to protect all parties - the students, the staff and the school.

### Professional Standards

Professional standards should be maintained in all electronic communication whether personal or work-related. This is for the protection of staff and to maintain the reputation of the school. Staff agree to comply with all school policies and these are available on the school website.

### Unacceptable Behaviour

In addition to illegal ICT use, the following is deemed unacceptable use or behaviour:

- promotion of any kind of discrimination
- promotion of racial or religious hatred
- threatening behaviour, including promotion of physical violence or mental harm
- viewing pornography
- any other behaviour which may be offensive to colleagues or could damage the reputation of the school
- using technology for personal financial gain, gambling, political purposes or advertising
- using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by SWGfL and / or the school
- uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions
- downloading or installing software without permission from the Network Manager
- revealing or publicising confidential or proprietary information (e.g. financial / personal, databases, usernames and passwords to school systems)
- creating or propagating computer viruses or other harmful files
- hacking into unauthorised areas or using unauthorised accounts
- undertaking deliberate activities that waste staff time or waste or damage network resources
- posting anonymous messages and/or forwarding spam
- using social networking sites, instant messaging or chat rooms on school computers or from within school unless used for the educational benefit of pupils and permission has been obtained from the Head Teacher
- using personal cameras or mobile phones to take images of children
- using personal mobile phones in front of children or in non-designated areas

### Monitoring

Ravenswood School accepts that the use of technology is valuable in teaching and learning. However, the misuse of technology can have a negative impact on staff, students and the reputation of the school.

- Checks are made on the use of school computers and the websites accessed from them. The use of social networking sites by staff may also be checked.
- The school will report any illegal website accessed through our connection.
- The school maintains the right to examine or delete any files held on its computer system.
- No school data (pictures, videos, documents etc) other than that which is freely accessible on the school website, is to be stored on any computer other than those owned by the school.

### Remote Access to School Systems

- School usernames and passwords must be kept secret.
- School data must not be viewed by other users, including family members.

<u>Use of devices not owned by the school:</u>

1. School accounts must not be added to the apps on personal mobile devices e.g. Teams, OneDrive or Seesaw apps.

2. School email may be added to the Outlook or native mail app on mobile phones (but this is not expected nor encouraged):
    - The user will be electronically forced to accept conditions including forcing a passcode to be used on the device and giving the school the power to remotely wipe data from the device.
    - The device must not be used by anyone else.
    - Change of ownership of the device should be reported to the Network Manager in advance. The school will take appropriate action to wipe the data. Users should also make appropriate arrangements for the device to be securely reset to prevent information being retained on the device.
    - Loss of the device must be immediately reported.
    - Attachments / files that may contain personal or confidential information must not be opened.
3. School Office 365 may be used through a browser on personal devices:
    - The browser must not be set to remember the password.
    - Attachments / files that contain personal or confidential information must not be downloaded to the device.
    - At the end of the session the school account must be logged out.
4. If a school attachment or file containing personal or confidential data has been downloaded to a device the user must make appropriate arrangements for the file to be securely deleted to prevent information being retained on the device.
5. When accessing school systems from a non-school device the user must ensure that the operating system regularly receives automatic updates. On Computers anti-virus software must be installed and receive regular updates.

**Sanctions**
Failure to comply with these guidelines will result in sanctions ranging from disciplinary procedures such as verbal and written warnings, through to dismissal or possible police involvement. Disciplinary action will also be taken if the actions of an employee adversely affect the reputation of a colleague or the school. Action will also be taken where such actions have been taken by an ex-employee. The school will report any illegal material discovered on its devices.

**Agreement**
All employees, contractors, temporary staff and volunteers who would like to be granted the right to use school computers are required to sign below to confirm their understanding and acceptance of this Agreement.

- I confirm I have read, understood and will comply with, the Online Safety Policy and the Data Protection and Information Sharing Policy, detailing the requirements for Online Safety and Information Governance at Ravenswood School.

Full name …… Class/Post ..……..……

Signed …… Date ……..……..…

**Access granted …… Date ……**

**Please return the completed form to the school Network Manager for approval.**
Personal data is stored on the school's computer network, and can be accessed by staff (who have the appropriate permissions) in school or over the internet. Any security breach must be immediately reported to the Network Manager, will be treated seriously and could become a child protection issue.

**Appendix E (1) KS3, KS4, P16 – Forms part of the Home-School Agreement**

# ICT Acceptable Usage Agreement for Pupils

We recognise the huge benefits of having access to the Internet and other technology. However, the internet can be unsafe for children and everybody needs to use the technology in an appropriate and responsible way in order to keep safe and secure.

**To use ICT in school you must agree to the rules below**

## Respecting Privacy

- I will not tell anyone my password.
- I will not log on as someone else.

## Looking After Equipment

- I will not harm or destroy equipment in school e.g. headphones, keyboards, computers.

## Using Websites

- I will not try to access any inappropriate or offensive websites, including chat rooms and social networking sites.
- If I find an unsuitable website I will tell my teacher.

## Using Email

**I will:**

- not send or encourage others to send rude or abusive messages.
- not send emails that contain anything which is inappropriate or upsetting to others and which could cause them distress.
- tell my teacher if I receive an electronic message or any attachments which are upsetting, inappropriate or abusive.

**I understand:**

- that school staff might check the emails I have sent and received and that messages containing something inappropriate will be shown to the Headteacher.
- that messages containing something illegal may be shown to the Head Teacher or even the police.

## Mobiles, Tablets, Electronic Games, Smart Watches and other technology

- These must not be brought in to school from home.

- If used as a calming device for journeys, I will hand it in to the school office when I arrive and collect it at home time.

**I will not:**

- send abusive, unkind or silly messages or pictures.
- use my own mobile device to access the internet at school.
- make unkind phone calls or ring and hang up.
- take photos, videos or sound clips of people or private information in school, without permission.

**Observing Copyright**

- I will check with my teacher before I email, publish or print something from the internet.

**Keeping Safe Online – remember the 'SMART' rules...**

**SAFE** - Keep safe by not giving out your full name, birthday or email address to anyone you don't trust or know online. Join-in with school e-safety activities.
**MEETING** - Meeting up with someone you have met online can be dangerous. They might not be who they say they are. If you must meet up tell your parents/carers and ask them to come with you.
**ACCEPTING** - Accepting e-mails, instant messenger messages or opening files from people you don't know might be dangerous. They might contain viruses or nasty messages!
**RELIABLE** - Someone online may be lying about who they are. Information on website may be untrue. Check information against other websites or books or ask an adult.
**TELL** - Tell your parent/carer or teacher if someone or something makes you feel uncomfortable or worried, or if you or someone else is being bullied by text or online.

## Appendix E (2) Social Communication

***Please read this agreement with your child.***


# Appendix F

## Teacher iPad agreement

Ravenswood will provide you with at least two Apple iPads for use by your students and staff team. You will be asked to sign to take responsibility for these iPads and must not loan them to other classes. Class sets of iPads may still be borrowed from the Network Manager when more than two are required. They should be booked through the iPad calendar which will also allow you to check their availability. Please include the Network Manager as a recipient of the booking request. Only adults are permitted to collect and return iPads.

Primary, KS3-4 and P16 iPads each have their own set of approved apps. You may not install new apps. To request the installation of new apps please email your request to the IT Subject Leader with a web link to the app's info page in the Apple App Store.

All iPads require a passcode to unlock them which you will be given. The passcode should not be shared beyond the class team. The passcode must not be changed.

Teachers may take iPads offsite if they plan to use them in a way that will benefit the school. Teachers can give written/email permission to support staff to take iPads offsite if it will benefit the school but overall responsibility for the device remains with the teacher. Non-school staff including family and friends are not permitted to use school iPads.

All usage must be in accordance with the ICT Acceptable Usage Agreement and the school's Online Safety Policy. High standards of data protection must be observed.

Examples of academic iPad usage (non-exhaustive):

- Clocks, timers and stop watches.
- Phonics apps.
- Photographs, videos, iMovie.
- Writing music through Garage Band.
- Siri / Safari – Internet research, Espresso.
- Maps, Beebots.
- Seesaw; used by staff through staff Seesaw accounts and pupils through student Seesaw accounts.

Ensure you logoff from school accounts like Office 365 and Seesaw before allowing other users to have the device.

You are responsible for:

- Ensuring appropriate supervision, minimising the risk of inappropriate usage or damage.
- Ensuring your iPads are charged.
- Locking your iPads away securely when not in use, and overnight.
- Immediately reporting loss, damage or inappropriate usage to the Headteacher. If necessary, the device will be remotely locked or wiped.

I agree to the conditions stated and accept responsibility for the iPads provided to my class.

| | | | | |
|---|---|---|---|---|
| iPad name: | | | | |
| iPad serial number: | | | | |

Class: _____

Print name: _____ Signature: _____

Date: _____

## Appendix G

Ravenswood School

**Personally-Allocated-iPad Agreement**

Ravenswood School provides Apple iPads to staff to enable them to carry out their job role more effectively. Please sign below to accept this iPad and agree to the following terms of use:

1. This iPad remains the property of Ravenswood School and is loaned to you for use within your job role.
2. The iPad must remain in your possession, should only be used by you and should be securely stored when not in use.
3. All iPad use must fully comply with the Ravenswood School ICT Acceptable Usage Agreement for Staff, Governors, Visitors and Community Users.
4. The iPad is connected to your school accounts so might have access to the personal information of pupils and staff. The iPad might also be used to store personal information such as picture and video images of pupils. This means you must fully comply with high standards of data protection.
5. This iPad may be configured with certain restrictions in place. You must not try to make changes to the device that are passcode protected. The passcode required to unlock the device has been configured to be at least 8 characters in length. You should choose your own passcode that is at least this length.
6. Loss or damage of the device should be immediately reported to the Headteacher. If necessary, the device will be remotely locked or wiped.
7. Insurance cover provides protection from the standard risks whilst the iPad is on the school site or in your home **but excludes** theft from your car or from other establishments. Should you leave the iPad unattended and it is stolen you will be responsible for its replacement and may need to claim this from your own insurance company.
8. This iPad is an expensive and fragile item and should be treated as such. It may be used in the classroom for teaching but any direct use by a pupil should only take place under direct supervision by you. Remember that personal information might be accessible on the device and you must fully comply with high standards of data protection.
9. If this iPad includes 4G internet access provided by the school you should try to keep 4G use to the minimum required to do your job effectively. 4G is only to provide internet access when you are out of range of school, your home or free public wi-fi access. Watching videos through a 4G connection is not advised. If you receive a message stating that you have used your 4G data allowance for the month you should inform the school's Network Manager.
10. Any connection cost incurred by accessing the internet from outside school, other than through school-provided 4G, is not chargeable to the school.
11. North Somerset Council CYPS policies and school policies regarding appropriate use and sharing information apply to this iPad. Use of the iPad must adhere to data protection, computer misuse and health and safety rules. Failure to do so may lead to disciplinary action.
12. This iPad will be checked annually for safety and for compliance with school policies. Outcomes will be reported to the Headteacher.
13. If you leave the employment of the school the iPad must be returned in good condition to the Network Manager before your official leaving date.

iPad Model:..... Serial No.: ……..

Name: .....

I have read this agreement and fully understand that I need to adhere to all elements.

Received by Signature: ..... Date: .....

Authorised by Network Manager: ..... Date: .....

## Appendix H

# Ravenswood School
# Loan Laptop Agreement

Ravenswood School will provide you with a laptop to enable you to carry out your job role more effectively. Please sign below to accept this laptop and agree to the following terms of use:

1. The laptop remains the property of Ravenswood School and is loaned to you for use within your job role.
2. The laptop must remain in your possession, should only be used by you and should be securely stored when not in use.
3. All laptop use must fully comply with the Ravenswood School ICT Acceptable Usage Agreement for Staff, Governors, Visitors and Community Users.
4. This laptop is an expensive and fragile item and should be treated as such. It may be used in the classroom for teaching but any direct use by a pupil should only take place under direct supervision by you. Remember that personal information might be accessible on the device and you must fully comply with high standards of data protection.
5. Insurance cover provides protection from the standard risks whilst the laptop is on the school site or in your home **but excludes** theft from your car or from other establishments. Should you leave the laptop is unattended and it is stolen you will be responsible for its replacement.
6. Loss or damage of the device should be immediately reported to the Headteacher.
7. Any telephone charges incurred by staff accessing the Internet remotely are not chargeable to the school.
8. North Somerset Council CYPS policies and school policies regarding appropriate use apply to this laptop. The user of the laptop must adhere to data protection, computer misuse and health and safety rules.
9. The laptop will be checked annually for safety and for compliance with school policies. Outcomes will be reported to the Headteacher.
10. If you leave the employment of the school the laptop must be returned in good condition to the Headteacher before your official leaving date.

Laptop Make & Model: ..... Serial No.: .....

Authorised by Headteacher: ..... Date: .....

Member of Staff: .....

Received by Signature: ..... Date: .....

**Appendix I**

# Home – School Laptop Agreement

## Academic year:

**Name of pupil:** **Date of birth:**
**Purpose: Learning Aid** **Owner: Ravenswood School**

Laptop make / model: Serial Number:

Ravenswood School would like to provide this pupil with a laptop to be used for school learning. To accept this agreement please sign below and return the form to school:

1. The parents/carers accept full responsibility for the laptop whilst it is at home.
2. They will look after the laptop by handling it carefully, keeping it at home and never leaving it in a car or public place.
3. The laptop will only be used as an aid to school learning.
4. Only apps relating to the main purpose will be installed.
5. The laptop will only be used by the pupil and not by other family members or friends.
6. If the laptop gets damaged, is lost or stolen whilst at home, the family will report this to the Headteacher.
7. The laptop will be checked regularly by the class team to make sure it is being used properly.
8. The school might ask for the laptop to be returned if this agreement is broken.
9. The laptop will be returned to school upon the request of the Headteacher or no longer attends Ravenswood School.

Pupil's name: Signature: _____

Parent/Carer's name: _____ Signature: _____

Headteacher's signature: _____

# Appendix J

# Ravenswood School Password Security

**Introduction**
The Network Manager is responsible for ensuring that the ICT network is as safe and secure as is reasonably possible and that:

- users can only access data to which they should have right of access
- no user should be able to access another's files without permission (except as allowed for monitoring purposes within school policies)
- access to personal data is securely controlled in line with the school Data Protection and Information Sharing Policy
- logs are maintained of access by users and of their actions while users of the system

A safe and secure username / password system is essential to ensure data security and the protection of staff and pupils. This policy applies to school accounts for logging on to school computers and Office 365 unless otherwise specified.

**Responsibilities**
The management of the password security is the responsibility of the Network Manager.

All users (adults and children) must keep their sign-in credentials secret. Adults should encourage pupils to keep their password secret to reduce the likelihood of pupils logging on as each other. Any device that can be used to access personal data must be locked or logged off when left unattended (even for very short periods) and set to auto lock if not used for five minutes. Users must not allow others to use their account except for the purposes of teaching or support. Where a pupil uses an interactive screen whilst the teacher is logged on, data protection remains the teacher's personal responsibility. Personal data is stored on the school's computer network, and can be accessed by staff (who have the appropriate permissions) in school or over the internet. Any security breach must be immediately reported to the Network Manager, will be treated seriously and could become a child protection issue. This is covered by the school's ICT acceptable usage agreements that all adults and pupils sign every year (Online Safety Policy: Appendices D & E).

**Training / Awareness**
It is imperative that staff and pupils keep their usernames and passwords secret.
Pupils will be made aware of the school's password security requirements:
- in ICT and online safety lessons
- through the ICT Acceptable Usage Agreement for Pupils (which is signed by all pupils annually)

Staff will be made aware of the school's password security requirements:
- through online safety training received as part of the induction process
- through the ICT Acceptable Usage Agreement for Staff, Governors, Visitors and Community Users (which is signed by all staff annually)
- through periodic online safety refresher training

**Policy Statements**
All users will have clearly defined access rights to school ICT systems. Details of the access rights held by groups of users will be recorded by the Network Manager and will be reviewed annually by the Online Safety Committee.

Pupils have individual accounts, but due to the nature of our pupils, passwords for school computers and Office 365 across the school should be organised as follows:

- Primary Department: Class passwords
- KS3 and KS4: Individual passwords where possible, otherwise class passwords
- Post 16: Individual passwords where possible, otherwise class passwords

Passwords for pupils will be set by the Network Manager according to department, as shown above, after liaison with the class teacher. Pupil passwords are usually set to never expire.

Passwords for staff will be set by the Network Manager and be forced to expire at first logon.

The following password rules describe the minimum level of security that applies to the use of staff passwords for logging on to school computers and these are electronically enforced:

- passwords expire and must be changed every 120 days the last five passwords cannot be re-used
- the password must be a minimum of 8 characters long and must include three of: uppercase character, lowercase character, number, special character
- accounts will “lock out” for 30 minutes following five successive incorrect log-on attempts
- passwords shall not be displayed on screen, and shall be securely hashed

Requests for staff password changes will only be taken from the member of staff concerned, their line manager or the Headteacher.

The School Information Management System (SIMS) contains personal and sensitive data and users of this system have a separate dedicated username and password. The system is hosted by Scomis and passwords are subject to the Scomis Password Policy (available online).

All staff laptops must be encrypted and a password or PIN required before they will start-up.

The administrator passwords for school ICT systems, used by the Network Manager, are regularly made available to the Headteacher. Administrator accounts should be set to require 2-factor authentication where possible.

**Audit / Monitoring / Reporting / Review**

The Network Manager will ensure that full records are kept of:

- Requests for staff password changes by anyone other than the user concerned
- User logons
- Security incidents related to this policy

In the event of a serious security incident, the police may request and will be allowed access to passwords used for encryption. Local Authority auditors also have the right of access to passwords for audit investigation purposes. User lists, User IDs and other security related information will be given the highest security classification and stored in a secure manner. These records will be reviewed by the Online Safety Committee annually. This policy will be regularly reviewed in response to changes in guidance and evidence gained from the logs.

# Appendix K

# Ravenswood School Filtering

### Introduction
The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will block all inappropriate material. It is therefore important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the circumstances at Ravenswood.

### Responsibilities
The responsibility for the management of the school's filtering in line with this policy will be held by the Network Manager. The Network Manager will keep logs of requests for filtering changes and the changes made. Changes to the SWGfL / school filtering service will be regularly reviewed by the Online Safety Committee.

All users have a responsibility to report immediately to the Online Safety Co-ordinator any infringements of the school's filtering policy of which they become aware or any sites that are accessed which they believe should have been filtered. If staff or pupils discover an unsuitable site, the URL, content, user who made the discovery, time it was discovered and device that was being used must be reported to the Network Manager. If appropriate, the Network Manager will filter the site and/or inform the Internet Service Provider in order for the site to be filtered for all schools. If the material reported is illegal the school will follow the procedure detailed in Appendix B.

Users must not attempt to bypass the filtering / security systems in place to prevent access to such materials. Requests to the Network Manager to check Facebook activity should be made by email from a member of the Senior Leadership Team (see 'Staff Proxy' section below).

### Education / Training / Awareness
Pupils will be made aware of the importance of filtering systems through the online safety education programme. They will also be warned of the consequences of attempting to bypass the filtering system.
Staff users will be made aware of the filtering systems through:

- the ICT Acceptable Usage Agreement, which they are required to sign annually
- the staff handbook
- online safety training received as part of the induction process
- online safety update sessions / weekly staff bulletin
- the school Online Safety Policy

Parents will be informed of the school's filtering policy through newsletters, online safety awareness sessions and through the school website.

### Staff Proxy
The SWGfL provides the 'staff proxy' service that allows the filtering administrator to bypass the school's filtering system. This will be used by the Network Manager to gain access to filtered websites for legitimate school purposes only, and in accordance with all school policies.

Examples of when this service might be used are:

- To log in to X (formally Twitter) to manage the school's X account
- In response to requests to check pupil or staff Facebook activity

The Network Manager will keep records of when and why the staff proxy has been used.

**Changes to the Filtering System**

Users who have accessed websites or have knowledge of others being able to access websites which they feel should be filtered will report this to the Online Safety Co-ordinator who will decide whether to make school-level changes. If it is felt that the site should be filtered at a higher level the Network Manager will report the site to the SWGfL. Requests to unfilter websites, specific web pages or videos should be made by email to the Network Manager and include full details of what the request is for and why it's being made.

**User Based Filtering (UBF)**

It will be the responsibility of the Online Safety Committee to decide whether any users/groups of users should be given access to websites that are usually filtered. An example was the decision made by the group to give staff access to YouTube. The granting of special access to particular websites and the use of these websites must be consistent with the aims of the school and its policies.

**Monitoring**

No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment as indicated in the school Online Safety Policy and the ICT acceptable usage agreements.

**Audit / Reporting**

Logs of filtering requests, changes to filtering and of filtering incidents will be made available to:

- the Online Safety Committee
- SWGfL / Local Authority on request

**Review**

The Filtering Policy will be reviewed by the Online Safety Committee in response to evidence provided by the audit logs and other monitoring that the school carries out. The school will work in partnership with the LA, DfE and the Internet Service Provider (South West Grid for Learning) to ensure systems to protect pupils are reviewed and improved.

# Appendix L

## Ravenswood School ICT Service Continuity Management

### Introduction

The use of ICT at Ravenswood School has increased to the point where it has become vital both to the delivery of the curriculum and to the management of the school. ICT systems therefore form a business-critical component of the institution.

The school will ensure that policies and procedures are in place to protect its digital data. In addition, planned recovery procedures will ensure recovery of data and systems is possible within a reasonable timeframe after hardware or system failure, caused by any number of unforeseeable events. Use of cloud systems is very important to the school and this adds a separate dimension to the risks that need to be minimised in order to maintain services.

### What is Service Continuity Management?

Service Continuity Management is a reactive and proactive process. It involves contingency planning for recovery in case an unforeseen disaster or event was to seriously affect or destroy the ICT service. It also involves risk analysis and the implementation of countermeasures to minimise the likelihood of such an event happening in the first place. The difference between Service Continuity Management and 'disaster recovery' is that Service Continuity Management includes a proactive element to reduce risk, whereas 'disaster recovery' is usually just the reactive part. Other benefits of Service Continuity Management include the following:

- The focus on service, rather than equipment, aligns the process with the overall school and ICT strategy, not just the technical support strategy
- Having a contingency plan reduces the impact on school activities of a medium- to long-term ICT outage
- It allows technical support to understand the importance and priority of ICT services within the school, which is beneficial day to day, not just in the event of a disaster

Therefore, Service Continuity Management is about maintaining continuity of service, not just the continuation of equipment. The school must consider all components of the ICT service, not just the hardware and software.

Similarly, the risks are not confined to the dramatic and remote-sounding examples of fire, flood and terrorist attack. There are many more commonplace possibilities such as a severed cable under a road, a leaking central-heating system, destructive software virus, transport difficulties affecting staff and loss of system password.

### ICT Service Continuity Recovery Plan

Ravenswood School will develop an ICT SCR Plan. The plan should consider the preparation for, response to and recovery from a disaster affecting all (or part) of the range of critical data held in the school's management information systems. The extent and sophistication of the plan will change over time according to the range of ICT systems and services that are in use, together with the amount and type of data stored. The ICT SCR Plan therefore needs to be regularly reviewed. Reviews will be made by the Online Safety Committee.

The school will follow these steps in producing its plan:

Step 1: Identify services and assets
E.g. **Service**: Internet **Assets**: Computer, software, LAN/WAN, communications link, contract with ISP

Step 2: Identify risks and threats
E.g. **Risk:** Loss of internal ICT services and / or assets **Threats:** Fire, flood, vandalism, weather damage, power failure, power surge, virus, accidental damage, environmental damage

Step 3: Make contingency plans
Use data collated in Step 2 to minimize risk where possible e.g. draw up 'pecking order' of which services to restore first, store copies of key documentation off site, document manual systems that can be used whilst ICT unavailable

Step 4: Document the recovery plan

**Characteristics of a successful implementation**

- Roles and responsibilities will be assigned
- Participants in service continuity management understand the process
- ICT services and equipment have been identified and documented
- Risks and threats to ICT services and equipment have been acknowledged
- Contingency plans have been drawn-up
- A Service Continuity Recovery Plan has been created
- The SCR Plan is updated as changes are made to ICT services
- The SCR Plan is as comprehensive as possible
- As far as possible, countermeasures to risks and threats have been implemented

**Current countermeasures to risks and threats to be incorporated into the plan**

1. **Security of information held on and systems running on school ICT equipment**
   The school Online Safety Policy, incorporating Password Security, Filtering, Data Protection and Information Sharing Policy all work together to cover many aspects of the security of the school's ICT systems and Information Governance. Additional aspects are covered as follows:
   - Each user with access to school servers will use a unique 'administrator' account
   - All school servers and PCs (including laptops) will be protected using appropriate anti-virus software e.g. Sophos
   - Users must report any virus warnings immediately to the Network Manager
   - All ICT devices over one year old must be tested annually for electrical safety
   - All servers in the school that are used to store school data and run information systems should be configured with a degree of disk redundancy (e.g. RAID 1 / 5 / 10)
   - An Uninterruptable Power Supply (UPS) should protect all servers from power fluctuations and outages
   - Servers should be located in secure areas and physical access restricted to authorized personnel only
2. **Backup and restoration procedures**
   - All servers in the school that are used to store school data and run information systems must be fully backed up to a suitable storage device at least once-a-week.

This backup must include the users' data together with any system information and programs that are needed to recover and access the data.

- Backups will use a minimum rotation of three individual data images to provide redundancy
- Backups will be encrypted
- Backup media will be securely stored at a remote location (e.g. the Annexe)
- Occasionally, the backups should be tested by the Network Manager to ensure that data restoration is possible
- The school has an ICT SCM plan with the roles and responsibility of staff clearly identified and the procedures to be followed clearly mapped

**3. System and Service Support**

- All software used on the school system will be appropriately licensed and a record kept of the licenses held by the school with supporting certificates where provided.
- All ICT systems used by the school will be supported through either or both of the following mechanisms:
  - Suitably trained support staff employed by the school
  - A service level agreement with an external ICT services provider
- The school has a hardware replacement plan in place that takes account of the projected life spans of systems and includes a contingency to cover system failure. For critical systems this will include provision for emergency system replacement or built-in redundancy capability.
- When servers are replaced, the Network Manager will ensure that the new servers are compatible with the system being replaced and that data can be successfully migrated.
- The school will plan for the movement of staff such that the ICT systems in use can still be supported should the current Network Manager cease to be available.

**4. Internet Use**

This is covered by the Online Safety Policy and acceptable usage agreements.

**Appendix M**

# Ravenswood School

# Online Safety Group Terms of Reference

While cybersecurity protects **devices** and **networks** from harm by third parties, Online Safety protects the **people** using them from harm by the devices and networks (and therefore third parties) through awareness, education, information and technology.

## 1. Purpose

To provide a consultative group that has wide representation from the school community, with responsibility for issues regarding online safety and the monitoring of the online safety policy including the impact of initiatives. The group will also be responsible for regular reporting to the Full Governing Body.

## 2. Membership

2.1. The online safety group will seek to include representation from all stakeholders.

The composition of the group should include:

- SLT member
- Child Protection/Safeguarding officer
- Teaching staff member
- Online safety coordinator
- Governor
- Parent / Carer
- ICT Technical Support staff
- Student representation – for advice and feedback.
  Pupil voice is essential in the make-up of the online safety group, but pupils would only be expected to take part in committee meetings where deemed relevant.

2.2. Other people may be invited to attend the meetings at the request of the Chairperson on behalf of the committee to provide advice and assistance where necessary.

2.3. Committee members must declare a conflict of interest if any incidents being discussed directly involve themselves or members of their families.

2.4. Committee members must be aware that many issues discussed by this group could be of a sensitive or confidential nature.

2.5. When individual members feel uncomfortable about what is being discussed they should be allowed to leave the meeting with steps being made by the other members to allow for these sensitivities.

## 3. Chairperson

The Committee should select a suitable Chairperson from within the group. Their responsibilities include:

- Scheduling meetings and notifying committee members;

- Inviting other people to attend meetings when required by the committee;
- Guiding the meeting according to the agenda and time available;
- Ensuring all discussion items end with a decision, action or definite outcome;
- Making sure that notes are taken at the meetings and that these with any action points are distributed as necessary

## 4. Duration of Meetings

Meetings shall be held every other term (3 times a year). A special or extraordinary meeting may be called when and if deemed necessary.

## 5. Functions

These are to assist the Online Safety Lead (or other relevant person) with the following:

- To keep up to date with new developments in the area of online safety
- To (at least) annually review and develop the online safety policy in line with new technologies and incidents
- To monitor the delivery and impact of the online safety policy
- To monitor the log of reported online safety incidents (anonymous) to inform future areas of teaching / learning / training.
- To co-ordinate consultation with the whole school community to ensure stakeholders are up to date with information, training and/or developments in the area of online safety. This could be carried out through:
    - Staff meetings
    - Student Council (for advice and feedback)
    - Governors meetings
    - Surveys/questionnaires for pupils, parents / carers and staff
    - Parents evenings
    - Website/Newsletters
    - Online safety events
    - Internet Safety Day / Week (annually held on second Tuesday in February)
    - Other methods
- To ensure that monitoring is carried out of Internet sites used across the school
- To monitor filtering / change control logs (e.g. requests for blocking / unblocking sites).
- To monitor the safe use of data across the school
- To monitor incidents involving cyberbullying for staff and pupils

## 6. Amendments

The terms of reference shall be reviewed annually from the date of approval. They may be altered to meet the current needs of all committee members, by agreement of the majority.

The above Terms of Reference for Ravenswood School have been agreed

Signed by (SLT): ..... Date: .....

Date for review: .....

**Appendix N**

**Legislation and guidance that should be considered when adhering to the Ravenswood School Online Safety Policy**

It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online. It is recommended that legal advice is sought in the advent of an online safety issue or situation. A useful summary of relevant legislation can be found at: https://reportharmfulcontent.com/when-should-you-go-to-the-police/

- Obscene Publications Act 1959 and 1964
- Protection of Children Act 1978
- Telecommunications Act 1984
- Protection of Children Act 1988
- Malicious Communications Act 1988
- Copyright, Designs and Patents Act 1988
- Computer Misuse Act 1990, amended by the Police and Justice Act 2006
- Criminal Justice and Public Order Act 1994
- Trade Marks Act 1994
- Defamation Act 1996
- Public Order Act 1986
- Protection from Harassment Act 1997
- Human Rights Act 1998
- Freedom of Information Act 2000
- Regulation of Investigatory Powers Act (RIPA) 2000
- Communications Act 2003
- Sexual Offences Act 2003
- Education and Inspections Act 2006 and 2011
- Racial and Religious Hatred Act 2006
- Safeguarding Vulnerable Groups Act 2006
- Equality Act 2010
- Protection of Freedoms Act 2012
- School Information Regulations 2012
- Criminal Justice and Courts Act 2015
- Serious Crime Act 2015
- Data Protection Act 2018
- Common Law Duty of Confidentiality
- Information Sharing Guidance