## Becket Primary School

# E-Safety, Social Media and Password Policy

## January 2019

*Becket Primary School acknowledges the assistance of North Somerset and SWGFL in providing content in this document.*

**PURPOSE**
This policy applies to all members of the school community (including staff, students, volunteers, parents / carers, visitors and community users) both in school and out of school. It is a statement of the aims, principles, strategies and procedures for e-safety throughout the school. Where this policy refers to 'staff' this also includes all volunteers, visitors and governors.

The policy provides the framework to nurture a safe digital community. 'Information Governance' refers to and encompasses the policies, procedures, processes and controls implemented to manage information. These support the school's immediate and future regulatory, legal, risk and operational requirements. Therefore the E-Safety, Social Media and Password Policy is part of the Information Governance suite and should be read in conjunction with our Data Protection and Information Sharing Policy, Safeguarding Policy and Whistle Blowing Policy.

This policy now includes, as Appendices;

- Staff, Governor and Volunteer Acceptable Use Policy
- Reception and KS1 Pupil Acceptable Use Policy
- KS2 Pupil Acceptable Use Policy

**RESPONSIBILITIES**

**The Governing Body shall:**

- Ensure this policy is implemented and procedures are in place that deal with the use of online activities and social networking sites.
- Ensure that all colleagues at the school have access to this policy and that colleagues including new colleagues are made aware of it.

**The Head Teacher shall:**

- Be familiar with this policy and guidelines and ensure that colleagues understand the policy and their own responsibilities.
- Ensure that colleagues at the school are aware of the risks of the use of social networking sites and the possible implications of the inappropriate use of them.
- Instigate disciplinary procedures where appropriate to do so.
- Seek advice where necessary from Human Resources on the approach to be adopted if they are made aware of any potential issue.

**Staff at the school shall:**

- Behave responsibly and professionally at all times in connection with the use of online activities and social networking sites.
- Ensure that all communication with pupils (including on-line communication) takes place within clear and explicit professional boundaries as set out in the DfE *Guidance for Safer Working Practice for Adults who work with Children and Young People in Education Settings* and preferably using school-based systems.
- Raise any concerns that any colleague(s) is/are not acting in accordance with this Policy with the Headteacher or e-safety leader.
- Act in accordance with the school's Whistleblowing Policy.
- Use their professional judgment and, where no specific guidance exists, take the most prudent action possible and consult with the Headteacher if they are unsure.
- Co-operate with management in ensuring the implementation of this policy.
- Respect the privacy and feelings of others.
- Keep a professional distance from pupils and ensure a clear separation of the private social lives of colleagues at the school and those of pupils.
- Report to their Headteacher or e-safety leader any occasions when a pupil attempts to involve them in on-line or social networking activity.

**PARENTS AND THIRD PARTIES ARE ENCOURAGED TO:**

- Raise any concerns that any member of staff at the school is/are not acting in accordance with this Policy with the Head Teacher.

WHAT IS E-SAFETY?

E-Safety refers to child protection and safeguarding of both children and adults in the digital world. It is about learning to understand and use technologies in a safe, positive way. It is also about supporting children and adults to develop safe online behaviours (both in and out of school).

**RISKS TO CHILDREN WHO USE THE INTERNET INCLUDE:**

- Exposure to inappropriate materials, for example, pornographic pictures and videos
- Physical danger and sexual abuse, for example, through 'grooming' by paedophiles
- Obsessive use of the internet and ICT, for example, addiction to video games
- Cyberbullying – persistent bullying through the digital medium
- Inappropriate or illegal behaviour, for example, exposure to hate mail or offensive images
- Copyright infringement, for example, the illegal sharing of music, pictures or documents

There are also risks to staff who use the internet.

E-Safety is largely concerned with internet communications. The internet is accessible from computers, laptops, tablets, mobile phones, games consoles and other devices like the iPod Touch and internet connected TV. Other communication technologies such as texting and phone calls are also covered by the term 'E-Safety'.

**WHAT IS SOCIAL MEDIA?**

Social media is defined as websites and applications that enable users to create and share content or to participate in social networking (The use of dedicated websites and applications to interact with other users, or to find people with similar interests to one's own).

Social media includes (but is not limited to) Facebook, Pinterest, Bebo, MySpace, Windows Live Spaces, MSN, Twitter, YouTube, blogs, wikis, forums, bulletin boards, chatrooms, multiplayer on-line gaming, virtual worlds, Linkedin, Flickr and Google+. The terms 'social media' and 'social networking' are interchangeable terms that cover every form of communication and interaction between people online.

**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 also enhances the school's management information and business administration systems.

**SCHOOL POLICY ON THE USE OF TECHNOLOGIES – PLEASE SEE PAGE 8 FOR AN OVERVIEW**

**INTERNET**

- Pupils will be taught what internet use is acceptable and what is not. They will be given clear objectives for internet use.
- School internet access will be filtered appropriate to the ability of the pupils to use it within school rules.
- 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 Acceptable User Policy for Pupils at the start of each key stage which must be countersigned by their parent or carer.

- All staff and visitors to school must read and sign the Acceptable User Policy for Staff, Governors and Volunteers before using any school ICT resources.
- 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.
- The school will ensure that use of internet derived materials by staff and pupils complies with copyright law.

Some internet activity eg accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities eg cyber-bullying would be banned and could lead to criminal prosecution. 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.

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts usage as follows:

| **USER ACTIONS** | | Acceptable | Acceptable at certain | Acceptable for nominated | Unacceptable | Unacceptable and illegal |
|---|---|---|---|---|---|---|
| **Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:** | **Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978** | | | | | X |
| | **Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.** | | | | | X |
| | **Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008** | | | | | X |
| | **criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986** | | | | | X |
| | **Pornography** | | | | X | |
| | **promotion of any kind of discrimination** | | | | X | |
| | **threatening behaviour, including promotion of physical violence or mental harm** | | | | X | |
| | **any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute** | | | | X | |
| **Using school systems to run a private business** | | | | | X | |
| **Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy** | | | | | X | |

| | | | | | |
|---|---|---|---|---|---|
| **Infringing copyright** | | | | X | |
| **Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)** | | | | X | |
| **Creating or propagating computer viruses or other harmful files** | | | | X | |
| **Unfair usage (downloading / uploading large files that hinders others in their use of the internet)** | | | | X | |
| **On-line gaming (educational)** | | X | | | |
| **On-line gaming (non educational)** | | | | X | |
| **On-line gambling** | | | | X | |
| **On-line shopping / commerce** | | | | X | |
| **File sharing** | | | | X | |
| **Use of social media** | | | | X | |
| **Use of messaging apps** | | | | X | |
| **Use of video broadcasting eg Youtube** | | | X | | |

**EMAIL**

- Staff and pupils may only use official school email accounts on the school system. Personal email accounts are not to be used.
- All emails sent must be professional in tone and content.
- Personal email accounts must not be used for communication between staff and students or parent/carers.
- Personal information (as defined in the Personal Data and Information Sharing Policy) must not be emailed to external email addresses from school email accounts as it is not secure.
- Care must be taken when emailing personal information from staff email addresses to www.n-somerset.gov.uk email addresses, and vice versa, as it is not secure.
- Pupils must have adult supervision whilst using email.
- Pupils must immediately tell a teacher if they receive offensive email.
- Pupils must not reveal personal details of themselves or others in email communication (such as address or telephone number).
- The forwarding of chain letters is not permitted.

**SOCIAL NETWORKING**
**ALL STAFF AT THE SCHOOL SHOULD FOLLOW THE FOLLOWING GUIDANCE / PROCEDURES:**

*Please note: if a member of staff at the school believes they will have any difficulty complying with any of the requirements below for whatever reason (for example, where they are related to a pupil), they should discuss the matter with the Head Teacher or e-safety leader. Failure to do so will be regarded as a serious matter.*

- Staff at the school must not access social networking sites for personal use via school information systems or using school equipment.
- Staff at the school must not accept pupils or past pupils as friends or use internet or web-based communication channels to send any personal messages to pupils – personal communication could be considered inappropriate and unprofessional and makes staff at the school vulnerable to allegations.
- Staff at the school must not accept parents as friends or use internet or web-based communication channels to send any personal messages to parents. The only exception is if the staff member can

prove they had a personal relationship with that parent before entering into a professional relationship with him or her.

- Any student-initiated communication, on-line friendships/friend requests must be declined and reported to the Head Teacher or designated safeguarding officer. If a staff receives messages on his/her social networking profile that they think could be from a pupil they must report it to their line Head Teacher and discuss whether it is appropriate for the staff to contact the internet service or social networking provider so that the provider can investigate and take the appropriate action.
- Staff at the school should not share any personal information with any pupil (including personal contact details, personal website addresses/social networking site details).
- Staff at the school should not place/post any material (or links to any material) of a compromising nature (that is, any material a reasonable person might find obscene or offensive (such as sexually explicit or unlawfully discriminatory material) including inappropriate photographs or indecent remarks or material relating to illegal activity) on any social network space.
- Staff at the school are advised not to write about their work but where a staff at the school chooses to do so:
    1. he/she should make it clear that the views expressed are his/hers only and do not reflect the views of the school/Local Authority (and all other guidelines in this policy must still be adhered to when making any reference to the workplace) and
    2. he/she must not disclose any information that is confidential to the school or disclose personal data or information about any individual/staff/pupil, which could be in breach of the Data Protection Act or disclose any information about the school/Local Authority that is not yet in the public arena
- Staff at the school should not post photographs of pupils under any circumstances and should not post photographs of other members or staff or parents without their express permission.
- Staff at the school should not make abusive/defamatory/undermining/derogatory remarks about the school/staffs/pupils/parents/governors or the Local Authority or post anything that misrepresents or could potentially bring the school/Local Authority into disrepute.
- Staff at the school should not disclose confidential information relating to their employment at the school.
- Staff at the school must not link their own sites to the school website or use the school's or the Local Authority's logo or any other identifiers on their personal web pages.
- If any staff at the school receives media contact regarding the content of their site or is offered payment for site content which relates to the school they must consult their Head Teacher.
- No staff at the school should use any internet/on-line resources to seek information on any pupil, parent or other staff member at the school other than for the purposes of legitimate monitoring of the usage of Social Networking sites by designated leaders or staff members.
- Staff at the school should not use social networking sites to seek to influence pupils regarding their own political or religious views or recruit them to an organisation of this kind using their status as a trusted adult to encourage this.

All communication via social networking sites should be made with the awareness that anything said, shown or received could be made available, intentionally or otherwise, to an audience wider than that originally intended. Staff at the school are strongly advised, in their own interests, to take steps to ensure that their on-line personal data is not accessible to anybody who they do not want to have permission to access it. For example, they are advised to check the security and privacy settings of any social networking site they subscribe to and set these to maximum. The e-safety leader can give further guidance on this.

The School reserves the right to take action to obtain the removal of any content posted by staff at the school which may adversely affect the reputation of the school (or any staff, governor, pupil or parent at the school) or put it at risk of legal action. Should the school decide to pursue this course of action, the advice of the Local Authority's marketing and Communications Team may be sought.

We would expect all former staff at the school to continue to be mindful of good children's safeguarding practice and of the school's reputation in using social networking sites.

The Governing Body does not discourage staff at the school from using social networking sites. However, all staff at the school should be aware that the Governing Body will take seriously any occasions where the services are used inappropriately. Instances of on-line bullying and harassment will be regarded as a serious matter and will be dealt with under the school's Disciplinary Policy. Any school staff who is being bullied or harassed on-line should report this to the Head Teacher.

In the event that this Policy is not followed or any instances of the inappropriate use of social networking sites are brought to the attention of the School, these may be investigated under the School's Disciplinary Policy and depending on the seriousness of the matter disciplinary action may be taken which may result in dismissal. A serious breach of the Policy may be regarded as gross misconduct, leading to summary dismissal.

**CHATROOMS AND INSTANT MESSAGING**

- The use of these facilities is not permitted in school.

**VIDEO CONFERENCING AND OTHER VIDEO COMMUNICATIONS**

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

**MOBILES, CAMERAS AND PORTABLE DIGITAL DEVICES**

**PUPILS:**

- Mobile phones brought into school by pupils must be handed-in to the class teacher at the start of the day. Other devices such as cameras, tablets, portable electronic games and media players should not be brought into school unless the Head Teacher has given permission.
- If a pupil is found to be in possession of one of these electronic devices, the Education Act 2012 gives authorised staff the right to search for such devices (in accordance with school policies) where they reasonably suspect that the data or files on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the school rules.
- The sending of abusive or inappropriate messages, emails or photos is forbidden.

**STAFF:**

- Use of personal devices in school such as computers, tablets, cameras and any other device with the functionality to take pictures, videos or make sound recordings, is not permitted. Exceptions to this rule are personal mobile phones and any device with specific written permission from the Head Teacher.
- Staff may only use personal mobile phones in areas where children are not present.
- Staff must not keep or use personal mobile phones in view of children.
- Staff must not use personal mobile phones during directed time unless permission has been given by the Head Teacher.
- The sending of abusive or inappropriate text messages is forbidden.
- Staff must not use personal devices to take images of children.
- Staff must not use personal devices to take any images, video or sound recordings in school.
- Staff must not use school devices to take inappropriate images of children or images of children in non-designated areas (non-designated areas include toilets and changing rooms).
- Staff are allowed to take digital photographs and video images to support educational aims, but follow guidance in the Acceptable User Agreement for Staff.
- Text messaging must not be used for communication between staff and parents.
- All staff have read and agreed to the principles of 'Safer Working Practice'.
- Members of staff who have requested to bring their own device to work for school use, have done so with agreement from the head teacher and full knowledge of the school technical support engineer, they adhere to the acceptable use and data protection policies.

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. The loss of an unencrypted memory stick containing the names of pupils would count.

- Encrypted memory sticks are provided for confidential data, this data will not be downloaded to home computers.
- Unencrypted memory sticks or portable hard disk drives may be used, but must not be used to store any data containing names of pupils or staff, or any photos of pupils.
- Photos should be downloaded from school digital cameras or iPads, at school, and onto school machines or network.
- 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 CD or DVD except:

- When archiving data to be stored securely at school.
- When sharing photos with parents (after a performance for example) but permission must be sought first from the Head Teacher or e-safety leader.
- With specific written permission from the Head Teacher.

**SCHOOL WEBSITE**

- The point of contact on the website should be the school address, email and telephone number. Staff or pupils' personal information will not be published.
- Each class teacher is responsible for updating his or her own class page and the page linked to his or her area of subject leadership. Staff should ensure this information is up to date, accurate and grammatically correct
- 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, particularly in association with photographs.
- The Head Teacher will delegate editorial responsibility to the deputy head teacher, to ensure that content is accurate and quality of presentation is maintained.

**EMERGING TECHNOLOGIES**

- Emerging technologies will be examined for educational benefit and a risk assessment carried out before use in school is allowed.

**OVERVIEW OF SCHOOL POLICY ON THE USE OF TECHNOLOGIES:**

| | Staff & other adults | | | | | Students / Pupils | | | |
|---|---|---|---|---|---|---|---|---|---|
| **Communication Technologies** | Allowed | Allowed at certain times | llowed for selected staff | Not allowed | | Allowed | Allowed at certain times | ed with staff permission | Not allowed |
| Mobile phones may be brought to school | X | | | | | | | X | |
| Use of mobile phones in lessons | | | | X | | | | | X |
| Use of mobile phones in social time | | X | | | | | | | X |
| Taking photos on mobile phones / cameras | | | | X | | | | | X |
| Use of other personal mobile devices eg tablets, gaming devices | | | | X | | | | | X |
| Use of personal email addresses in school, or on school network | | | | X | | | | | X |
| Use of school email for personal emails | | | | X | | | | | X |
| Use of messaging apps | | | | X | | | | | X |
| Use of social media on school devices | | | | X | | | | | X |
| Use of blogs | | | X | | | | | | X |

**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 mobiles phones, gaming or the internet, they can often feel very alone and, a once previously 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 is provided by SWGfL .
- Any change requests would need to be managed by the head teacher or e-safety leader.
- Any changes to the current filtering would need to be undertaken with explicit permission of the head teacher and e-safety committee.
- 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.
- 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 E-Safety Leader and record this in the incident report log. If appropriate, the E-Safety Leader will inform the Internet Service Provider in order for the site to be blocked.

**MONITORING**

- Logs of internet activity will be regularly checked.
- Pupil and staff files stored on school computers will be regularly checked.
- Pupil and staff emails will be regularly checked.
- Pupil and staff use of social networking websites will be regularly checked.
- Illegal misuse will be dealt with in accordance with procedure.

**SCHOOL ICT AND DATA SECURITY**

- The school Data Protection and Information Sharing Policy applies.
- Users must not share their user account details.
- Users must lock their laptop/ computer / iPad if leaving it unattended.
- Administrative data sent over the internet will be encrypted or otherwise secured.
- Unapproved system utilities and executable files are not permitted on school equipment.
- 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.
- Loss of personal data must be immediately reported to the Head Teacher, as an Information Risk Incident.
- Virus protection updates and system updates for PCs will be regularly installed.
- The school password requirements apply. These are:

**STAFF PASSWORDS:**

- All staff users will be provided with a username and password by the bursar who will keep an up to date record of users and their usernames.
- The password should be a minimum of 8 characters long and should include three of – uppercase character, lowercase character, number, special characters.
- Must not include proper names or any other personal information about the user that might be known by others.
- Temporary passwords e.g. used with new user accounts or when users have forgotten their passwords, shall be enforced to change immediately upon the next account log-on.

- Passwords shall not be displayed on screen, and shall be securely hashed (use of one-way encryption).
- Teachers should take care not to display passwords when using the interactive whiteboard.
- Passwords should be different for different accounts, to ensure that other systems are not put at risk if one is compromised.
- Passwords should be changed regularly.
- Passwords should be different for systems used inside and outside of school.

**PUPIL PASSWORDS**

- When relevant, pupils will be provided with a username and password by their class teacher who will keep an up to date record of users and their usernames.
- Pupils will be taught the importance of password security.
- The complexity (i.e. minimum standards) will be set with regards to the cognitive ability of the children.

**TRAINING / AWARENESS**

It is essential that users should be made aware of the need for keeping passwords secure, and the risks attached to unauthorised access / data loss. This should apply to even the youngest of users, even if class log-ons are being used.

**POLICY ENFORCEMENT**

The E-Safety Leader will ensure that the E-Safety, Social Media and Password Policy is implemented and compliance with the policy monitored.

**SCHOOL SANCTIONS**

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures which may be as outlined overleaf:

**PUPILS** **POSSIBLE ACTIONS / SANCTIONS**

| Incidents: | Refer to class teacher | Refer to e-safety Leader | Refer to Headteacher | Refer to Police | Refer to technical support staff for action re filtering / security etc | Inform parents / carers | Removal of network / internet access rights | Warning | Further sanction |
|---|---|---|---|---|---|---|---|---|---|
| **Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).** | | X | X | X | X | X | X | X | X |
| Unauthorised use of non-educational sites during lessons | X | | | | | | | X | |
| Unauthorised use of mobile phone / digital camera / other mobile device | X | X | | | | X | | X | |
| Unauthorised or inappropriate use of social media / messaging apps / personal email | X | X | X | | | X | | X | |
| Unauthorised downloading or uploading of files | X | X | | | X | X | | X | |
| Allowing others to access school network by sharing username and passwords | X | X | | | | | | X | |
| Attempting to access or accessing the school network, using another student's / pupil's account | X | X | | | | | | X | |
| Attempting to access or accessing the school / academy network, using the account of a member of staff | X | X | | | | | | X | |
| Corrupting or destroying the data of other users | X | | | | | | | X | |
| Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature | X | X | X | | | X | X | X | |
| Continued infringements of the above, following previous warnings or sanctions | X | X | X | | | X | X | X | X |
| Actions which could bring the school into disrepute or breach the integrity of the ethos of the school | X | X | X | | | X | X | X | X |
| Using proxy sites or other means to subvert the filtering system | X | X | | | X | X | X | X | |
| Accidentally accessing offensive or pornographic material and failing to report the incident | X | X | X | | X | X | | X | X |
| Deliberately accessing or trying to access offensive or pornographic material | X | X | X | X | X | X | X | X | X |
| Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act | X | X | | | | | | X | X |

**STAFF** **POSSIBLE ACTIONS / SANCTIONS**

| Incidents: | Refer to e-safety lead | Refer to Headteacher | Refer to Local Authority / HR | Refer to Police | Refer to Technical Support Staff for action | Warning | Suspension | Disciplinary action |
|---|---|---|---|---|---|---|---|---|
| **Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).** | X | X | X | | X | X | X | X |
| Inappropriate personal use of the internet / social media / personal email | X | X | | | | X | | X |
| Unauthorised downloading or uploading of files | X | | | | X | | | |
| Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account | X | X | | | | X | | X |
| Careless use of personal data eg holding or transferring data in an insecure manner | X | X | | | | X | | X |
| Deliberate actions to breach data protection or network security rules | X | X | X | | | X | | X |
| Corrupting or destroying the data of other users or causing deliberate damage to hardware or software | X | X | | | | X | | X |
| Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature | X | X | X | | | X | | X |
| Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils | X | X | X | | | | | X |
| Actions which could compromise the staff member's professional standing | X | X | | | | X | | X |
| Actions which could bring the school into disrepute or breach the integrity of the ethos of the school | X | X | | | | X | | X |
| Using proxy sites or other means to subvert the school's filtering system | X | X | | | X | X | | |
| Accidentally accessing offensive or pornographic material and failing to report the incident | X | X | | | X | | | |
| Deliberately accessing or trying to access offensive or pornographic material | X | X | X | X | X | X | X | X |
| Breaching copyright or licensing regulations | X | X | | | | X | | |
| Continued infringements of the above, following previous warnings or sanctions | | | | X | | | X | X |

**COMPLAINTS**

- Responsibility for handling incidents of internet misuse will be taken by the E-Safety Leader.
- Any complaint about staff misuse of ICT must be referred to the Head Teacher.
- 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.
- Parents and pupils will need to work in partnership with staff to resolve issues.
- There may be occasions when discussions will be held with the police support services to establish procedures for handling potentially illegal issues.
- Where possible the school will liaise with local organisations to establish a common approach to e-safety.

**EDUCATION**

**EDUCATION & TRAINING: STAFF AND GOVERNORS**

- All new staff and governors are encouraged to receive e-safety training as part of their induction programme.
- All new staff, visitors and governors are asked to read this policy and sign the Acceptable User Policy as part of their induction.
- The E-Safety Leader receives regular updates through attendance at SWGfL, CEOP, LA training sessions and by reviewing regular e-safety updates from the local authority.
- This E-Safety Policy and its updates are shared and discussed in staff meetings. Updates are provided to all staff.
- The E-Safety Leader 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 e-safety is therefore an essential part of the school's e-safety provision. Pupils need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

- E-safety is included in every unit of the computing Scheme of Work.
- Key e-safety messages are reinforced annually to link in with Safer Internet Day.
- Pupils are helped to understand and act in accordance with the Acceptable User Policy for Pupils.
- The Acceptable User Policy for Pupils is displayed in the ICT suite, on the laptop trollies and on the school website.
- E-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.
- 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 Acceptable User Policy for Pupils.

**EDUCATION: PARENTS/CARERS**

Parents and carers may have only a limited understanding of e-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 e-safety risks at home, reinforcing key messages about e-safety and regulating their home experiences. The school supports parents to do this by:

- Providing regular newsletter and website updates on e-safety.
- Proving information leaflets to parents when requested.
- Inviting parents to attend activities such as evening e-safety sessions.

- Promoting e-safety.
- Drawing parents' attention to the school E-Safety, Social Media and Password Policy in newsletters, the school website and during e-safety events such as Safer Internet Day.
- Asking parents to read through the Acceptable User Policy for Pupils with their child and co-sign the agreement.
- Sensitive handling of internet issues to inform parents without undue alarm.

**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 E-Safety Leader 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 e-safety policy has been developed, and will be monitored, by our school e-Safety Committee which comprises:

- A member of the Senior Leadership Team
- E-Safety Leader
- Computing Leader
- E-Safety Governor
- Teaching and Support staff
- Parent representatives
- Pupil representatives

The school will monitor the impact of the policy using:

- Logs of reported incidents
- SWGfL monitoring logs of internet activity
- Regular checks on school emails, users' files, browsing history and staff and pupil use of social networking websites

The policy will be reviewed immediately where monitoring data shows a need. The policy will also be reviewed at least every three years.

Next review date is **March 2020**

**Signed**

**Heat Teacher …… Date……..**

**Chair of Governors: ……. Date……..**