



South Wingfield

PRIMARY SCHOOL

Online Safety Policy

Background / Rationale

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning.

Children and young people should have an entitlement to safe internet access at all times. The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. The aim of this policy is to help to ensure safe and appropriate use of these technologies. The development and implementation of this strategy involves all the stakeholders in a child's education from the headteacher and governors to the senior leaders and classroom teachers, support staff, parents, members of the community and the pupils themselves.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement. However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is used in conjunction with other school policies (e.g. behaviour, antibullying and child protection policies).

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

The school must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The e-safety policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents / carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

Development / Monitoring / Review of this Policy

- This e-safety policy has been developed by a working group made up of: ➤
 - ICT Co-ordinator
 - Headteacher
 - Senior Leaders ➤ ICT Technician
 - Governors

- Consultation with the whole school community has taken place through the following:
 - Staff meetings
 - INSET Day
 - Governors Meetings
 - Parents Evenings
 - School website
 - Newsletters
 - School Council Meetings

Version Control

Version number 5

Schedule for Development / Monitoring / Review

The implementation of this e-safety policy will be monitored by the:

- ICT Coordinator
- E-Safety Governor
- ICT Technician
- Headteacher
- Class Teachers
- Teaching Assistants

Monitoring will take place regularly. The Governing Body will receive a report on the implementation of the e-safety policy generated by the monitoring group (which will include anonymous details of e-safety incidents) annually prior to the review of the policy.

The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be July 2023.

Should serious e-safety incidents take place, the following external persons/agencies should be informed: LA ICT Manager, LA Safeguarding Officer and Police Commissioner's Office.

The school will monitor the impact of the policy using:

- Logs of reported incidents (written by resident ICT Technician and ICT Coordinator)
- Monitoring logs of internet activity (including sites visited)
- Surveys / questionnaires of pupils (eg Ofsted "Tell-us" survey / CEOP ThinkUknow survey)

Scope of the Policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents/carers and visitors) who have access to and are users of school ICT systems, both in and out of school.

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate E-safety behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the roles and responsibilities for e-safety of individuals and groups within the school.

Governors:

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors / Governors

Sub Committee receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of ESafety Governor.

The role of the E-Safety Governor will include:

- regular meetings with the E-Safety Coordinator / Officer
- regular monitoring of e-safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Governors committee / meeting

Headteacher and Senior Leaders:

- The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for esafety will be delegated to the ICT co-ordinator.
- The Headteacher / Senior Leaders are responsible for ensuring that the ICT co-ordinator and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- 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 e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team / Senior Management Team will receive regular monitoring reports from the ICT co-ordinator.
- The Headteacher and Deputy Headteacher should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

ICT Coordinator:

- Leads the e-safety committee.
- Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- Provides training and advice for staff.
- Liaises with the Local Authority.
- Liaises with school ICT technician.
- Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments.
- Meets regularly with E-Safety Governor to discuss current issues, review incident logs and filtering / change control logs.
- Attends relevant meeting / committee of Governors.
- Reports regularly to Senior Leadership Team.

ICT Technician:

The ICT Technician is responsible for ensuring:

- that the school's ICT infrastructure is secure and is not open to misuse or malicious attack.
- that the school meets the e-safety technical requirements outlined in the Acceptable Usage Policy and any relevant Local Authority ESafety Policy and guidance.
- that users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed.
- that the appropriate company is informed of issues relating to the filtering applied.
- that the school's filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.
- that he / she keeps up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant.
- that the use of the network / Virtual Learning Environment (VLE) / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the ICT Co-ordinator / Headteacher for investigation, action or sanction.
- that monitoring software / systems are implemented and updated as agreed in school policies.

Teaching and Support Staff:

Are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices.
- they have read, understood and signed the school Staff Acceptable Use Policy.
- they report any suspected misuse or problem to the ICT Co-ordinator, ICT Technician or Headteacher.
- digital communications with pupils (email / Virtual Learning Environment (VLE) / voice) should be on a professional level and only carried out using official school systems.
- e-safety issues are embedded in all aspects of the curriculum and other school activities.
- pupils understand and follow the school e-safety and acceptable use policy.
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- they monitor ICT activity in lessons, extra curricular and extended school activities.
- they are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices.
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Child Protection Co-ordinator:

Should be trained in e-safety issues and be aware of the potential for serious child protection issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

E-Safety Committee:

Members of the E-safety committee will assist the ICT Co-ordinator with:

- the production / review / monitoring of the school e-safety policy / documents.
- the production / review / monitoring of the school filtering policy.

Students / pupils:

- are responsible for using the school ICT systems in accordance with the Pupil and Parent/Carer Acceptable Use Policy, which they will be expected to sign before being given access to school systems.
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school.

Parents / Carers:

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national / local e-safety campaigns / literature.

Parents and carers will be responsible for:

- endorsing (by signature) the Pupil and Parent/ Carer Acceptable Use Policy.
- accessing the school website in accordance with the Pupil and Parent/ Carer Acceptable Use Policy.

Policy Statements

Education – pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

E-Safety education will be provided in the following ways:

- A planned e-safety programme should be provided as part of ICT / PHSE / other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school.
- Key e-safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities.
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.

- Pupils should be helped to understand the need for the Pupil and Parent/ Carer Acceptable Use Policy and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet. ➤ Rules for use of ICT systems / internet will be posted in all rooms.
- Staff should act as good role models in their use of ICT, the internet and mobile devices.

Education – parents / carers

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide". (Byron Report).

The school will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters and the school web site.
- Parents evenings

Messages to the public around e safety should also be targeted towards grandparents and other relatives as well as parents. Everyone has a role to play in empowering children to stay safe while they enjoy these new technologies, just as it is everyone's responsibility to keep children safe in the non-digital world.

Education & Training – Staff

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy.

Training will be offered as follows:

□ A planned programme of formal e -safety training will be made available to staff. An audit of the e-safety training needs of all staff will be carried out regularly. It is expected that some staff will identify e-safety as a training need within the performance management process.

- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policies.
- The ICT Coordinator will receive regular updates through attendance at LA meetings, training and by reviewing guidance documents released by BECTA.
- This E-Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The ICT Coordinator will provide advice / guidance / training as required to individuals as required.

Training – Governors

Governors should take part in e-safety training / awareness sessions, with particular importance for those who are members of any sub committee / group involved in ICT / e-safety / health and safety / child protection.

This may be offered in a number of ways:

- Attendance at training provided by the Local Authority or other relevant organisation.
- Participation in school training / information sessions for staff or parents.

Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their esafety responsibilities:

- School ICT systems will be managed in ways that ensure that the school meets the e-safety technical requirements outlined in the Acceptable Usage Policies and any relevant Local Authority E-Safety Policy and guidance.
- There will be regular reviews and audits of the safety and security of school ICT systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the ICT Technician and will be reviewed, at least annually, by the E-Safety Committee.
- All users will be provided with a username and password by the ICT Technician who will keep an up to date record of users and their usernames. Users will be required to change their password if security issues arise.
- The “administrator” passwords for the school ICT system, used by the ICT Coordinator and ICT technician must also be available to the Headteacher or other nominated senior leader and kept in a secure place.
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- The school maintains and supports the managed filtering service provided by KCom as recommended by Derbyshire County Council.
- In the event of the ICT Technician (or other person) needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher.
- Any filtering issues should be reported immediately to KCom.
- Requests from staff for sites to be removed from the filtered list will be considered by the ICT Coordinator, ICT Technician and Headteacher. If the

request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the E-Safety Committee.

- School ICT technical staff regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy.
- An appropriate system is in place for users to report any actual / potential esafety incident to the ICT Coordinator or ICT Technician. Incidents are recorded in the E-Safety Incident Log.

- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.
- “Guests” such as supply and trainee teachers should follow the Teachers and Adults Acceptable Use Policy. An agreed policy is in place regarding the downloading of executable files by users. (Acceptable Use Policy).
- An agreed policy is in place (Acceptable Use Policy) that allows staff to install programmes on devices.
 - An agreed policy is in place (Acceptable Use Policy) regarding the use of removable media (e.g. memory sticks / CDs / DVDs) by users on school devices.
- The school infrastructure and individual workstations are protected by up to date virus software.
 - Personal data can not be sent over the internet or taken off the school site unless safely encrypted or otherwise secured. (Acceptable Use Policy)

Curriculum

E-safety should be a focus in all areas of the curriculum and staff should reinforce esafety messages in the use of ICT across the curriculum.

- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that 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 should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the ICT Technician temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need. Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

Use of digital and video images - Photographic, Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. T

here are many reported incidents of employers carrying out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing images on the internet e.g. on social networking sites.
- Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.

- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.
- Pupil's work can only be published with the permission of the pupil and parents or carers.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

Following a number of "high profile" losses of personal data by public organisations, schools are likely to be subject to greater scrutiny in their care and use of personal data.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, USB stick or any other removable media:

- the data must be encrypted and password protected
- the device must be password protected (many memory sticks / cards and other mobile devices cannot be password protected)
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning.

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

- The official school email service may be regarded as safe and secure and is monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems.
- Users need to be aware that email communications may be monitored.
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and pupils or parents/carers (email or website) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications as outlined in the Acceptable Use Policy.
- Pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.

- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Unsuitable / inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other ICT systems. Other activities e.g. 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 Acceptable Use Policy as inappropriate in a school context and that users should not engage in these activities in school or outside school when using school equipment or systems.

Responding to incidents of misuse

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse appears to involve illegal activity i.e.

- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

The ICT Coordinator and Headteacher must be informed immediately. They will then take relevant action in accordance with Derbyshire County Council Guidelines and the incident will be reported to the police and any evidence preserved.

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. More than one member of staff will be involved in the investigation which should be carried out on a "clean" designated computer.

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.