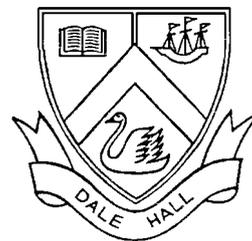


# DALE HALL COMMUNITY PRIMARY SCHOOL ICT ACCEPTABLE USE/ONLINE SAFETY POLICY



**This policy should be carried out in the context of and in conjunction with Dale Hall CP School's Safeguarding Policy.**

## **1. Introduction**

ICT is an essential part of learning and teaching, as well as everyday life, in the 21st Century. ICT covers a wide range of resources including web-based and mobile learning. At Dale Hall Community Primary School we encourage staff and learners to use ICT effectively and develop the use of ICT as essential life skills.

This policy is inclusive of both fixed and mobile internet; technologies provided by the school and technologies owned by pupils and staff, but brought onto school premises.

Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. At Dale Hall Community Primary School we use it to raise educational standards, to promote pupil achievement, to support the professional work of staff, to enhance the school's management information and business administration systems and to communicate with parents.

We believe that staff and pupils will benefit from the breadth and depth of information accessible to them. Benefits include:

- access to worldwide resources and research materials
- educational and cultural exchanges between pupils worldwide (Skype for instance)
- access to experts in many fields for both staff and pupils
- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- collaboration with support services, professional associations and colleagues;
- improved access to technical support including remote management of networks and automatic system updates;
- exchange of curricular and administration data (i.e. between colleagues, LA and DFE)

Due to the nature of the Internet and the range of information available through it, it is essential that a policy is in place to ensure the safety and well-being of all our staff and learners. We understand the responsibility to educate our pupils on e-Safety issues; teaching them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom. Access to the school's ICT network and use of ICT facilities owned by the school, including access to the Internet, are conditional on observance of this policy.

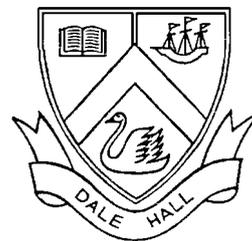
The policy was last reviewed on **20<sup>th</sup> November 2018** and will be reviewed annually by the Learning and Achievement Committee.

## **2. Aims of this Policy**

- allow all users access to school ICT resources and use of the Internet for educational and administrative purposes.
- provide a mechanism by which staff and pupils are protected from Internet sites, information, and individuals that would undermine the principles and aims of the school.

# DALE HALL COMMUNITY PRIMARY SCHOOL

## ICT ACCEPTABLE USE/ONLINE SAFETY POLICY



- provide rules which are consistent, and in agreement with the Data Protection Act 1998, Computer Misuse Act 1990 and other legislation relevant to the use of computers and electronic data in schools.
- provide rules that are consistent with the acceptable procedures commonly used on the Internet, including those associated with netiquette.
- provide rules relating to the use of computers and ICT facilities in school, which are consistent with the general policies of the school.

### **3. The Technologies**

ICT has an all-encompassing role within the lives of children and adults. New technologies are enhancing communication and the sharing of information. Current and emerging technologies used in school or used outside of school by children include:

- Websites
- Learning Platforms and Virtual Learning Environments
- E-mail and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/ Smart phones with text, video and/ or web functionality
- Tablets
- Other mobile devices with web functionality

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

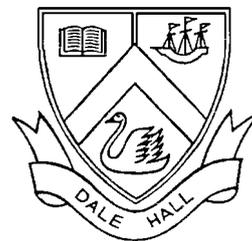
### **4. Roles and Responsibilities**

ICT Acceptable use/Online Safety is recognised as an essential aspect of strategic leadership in this school and the Headteacher, with the support of Governors, aims to embed safe practices into the culture of the school.

- The Headteacher ensures that the Policy is implemented and compliance with the Policy monitored.
- Governors need to have an overview understanding of acceptable use/ Online safety issues and strategies at this school.  
The school will actively take all reasonable precautions to prevent pupils being exposed to undesirable materials. The school has invested in hardware and software infrastructures to reduce risks associated with the Internet. All Internet access is filtered through a proxy server to screen out undesirable sites at source. However, if staff or pupils discover unsuitable sites or undesirable material, they will know that they should switch off the monitor, not the computer, and report the incident to the nearest teacher or the Headteacher who will report the URL (address), time, date and content to the Internet Service Provider. Any material that the school believes is illegal must be referred to the LA and take their advice. The security of the school ICT systems will be reviewed regularly. Virus protection is installed and will be updated regularly. The network manager will review system capacity regularly. The school is also committed to protecting its staff, learners, and itself from illegal or damaging actions by individuals, either knowingly or unknowingly. This requires a

# DALE HALL COMMUNITY PRIMARY SCHOOL

## ICT ACCEPTABLE USE/ONLINE SAFETY POLICY



team effort involving the participation and support of all staff who deal with information and/or information systems. It is the responsibility of every staff user to read and understand these guidelines, and to conduct their activities accordingly.

- All teachers are responsible for promoting and supporting safe behaviours in their classrooms and following school Online safety procedures.( See Appendices 1 and 5).

### 5. Using the Internet in class or at home

- **Internet enhanced learning**

- pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use. They are taught about cyberbullying and how to combat it
- internet access will be planned to enrich and extend learning activities
- staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity
- pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation

- **Evaluating Internet content**

- if staff or pupils discover unsuitable sites, the URL (address), time, date and content must be reported to the Internet Service Provider via the Headteacher
- staff ensure that the use of Internet derived materials complies with copyright law.
- pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.
- the evaluation of on-line materials is a part of every subject.

- **E-mail**

Whole-class or group e-mail addresses should be used at Key Stage 2 and below. Pupils must not reveal personal details of themselves or others in e-mail communication.

- **Social networking and personal publishing**

- pupils are advised never to give out personal details of any kind which may identify them or their location. Examples would include real name, address, mobile or landline phone numbers, academy, IM address, e-mail address, names of friends, specific interests and clubs etc.
- pupils are advised not to place personal photos on any social network space. They consider how public the information is and consider using private areas. Advice is given regarding background detail in a photograph which could identify the pupil or his/her location eg. house number, street name, academy, shopping centre.
- pupils are advised of the laws regarding social networking sites and are told they should not be on social media sites such as Facebook if they are under age
- pupils are advised on what to do if they have an online safety concern

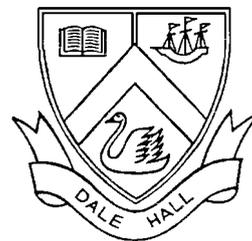
- **Videoconferencing /Skype**

Videoconferencing/skyping with another school is a challenging activity with a wide range of learning benefits. It is supervised by the teacher. When video conferencing or skyping with another school, parental permission is obtained.

### 6. Conditions of Use

# DALE HALL COMMUNITY PRIMARY SCHOOL

## ICT ACCEPTABLE USE/ONLINE SAFETY POLICY



Users are responsible for their behaviour and communications. Schools hold personal data on learners, staff and other people to help them conduct their day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, and potentially damage the reputation of the school. This can make it more difficult for your school to use technology to benefit learners. Everybody in the school has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them. Staff will be expected to use the resources for the purposes for which they are made available.

Users are to take due care with the physical security of hardware they are using. Staff will report any misuse of the network to the Headteacher. Users are expected to utilise the network systems in a responsible manner. Appendices 2 and 3 provide some guidelines on the matter.

All users are required to follow the conditions laid down in the policy.

These networked resources are intended for educational purposes, and may only be used for legal activities consistent with the rules of the school. Any use of the network that would bring the name of the school into disrepute is not allowed.

### **7. Unacceptable Use**

Any breach of the conditions may lead to withdrawal of the user's access, monitoring and or retrospective investigation of the users' use of services, and in some instances could lead to criminal prosecution. Any breach of the conditions will also be considered a disciplinary matter.

For examples of unacceptable use see Appendix 4.

Any malicious attempt to harm or destroy any equipment or data of another user or network connected to the school system will result in loss of access, disciplinary action and, if appropriate, legal referral. This includes the creation or uploading of computer viruses.

### **8. Personal data**

Personal data is recorded, processed, transferred and made available according to the Data Protection Act 1998.

### **9. Risk Assessment**

In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users 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. The school cannot accept liability for the material accessed, or any consequences of Internet access.

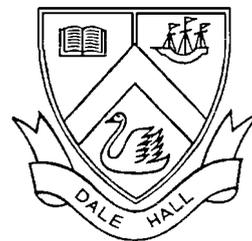
Methods to identify, assess and minimise risks will be reviewed regularly.

### **10. Physical Security**

Staff users are expected to ensure that portable ICT equipment such as laptops, digital, still and video cameras are secure when they are not being used.

# DALE HALL COMMUNITY PRIMARY SCHOOL

## ICT ACCEPTABLE USE/ONLINE SAFETY POLICY



### **11.School Website and Facebook**

The copyright of all material produced by the school for display on the school's web pages belongs to the school. Permission to reproduce any other material will be sought and obtained, from the copyright owner.

The contact details for the school will include only the school's postal address, e-mail address and telephone number. No personal information of staff or pupils will be published. The school will not publish photographs of pupils without a parent or carer's permission, in line with the school's photography policy. A pupil's name will not be used in association with photographs.

The school has a Facebook page which is regularly update by staff. It will have children's learning on but children will not be identifiable in photos. Staff should be wary of 'liking' the page from their personal accounts.

### **12.Mobile Phones**

The aim of this section is to promote safe and appropriate practice through establishing clear and robust acceptable use guidelines.

We understand that pupils may bring mobile phones to school. The pupils hand these in to the school office where they are kept until the end of the day. Phones should not be on when on the school premises.

As a general rule staff will not make or receive calls or texts during lesson time or meetings. Phones will be kept on silent during these times. This is to avoid distraction and disruption during lessons and meetings. Phones will not be used in a space where children are present e.g. classroom, playground. This will avoid adults putting themselves into compromising situations which could be misinterpreted and lead to possible allegations. There may be exceptional circumstances when staff need to keep their phones on as a necessary reassurance . Such use will be for an agreed limited period until issues or concerns leading to the exceptional circumstance request have been resolved. It is ensured that at all times the school landline is available for emergency or urgent contact. If children (year 6 only) bring mobile phones into school they must be handed in to the school office at the beginning of the day and collected at the end. They must not be switched on, on the school premises.

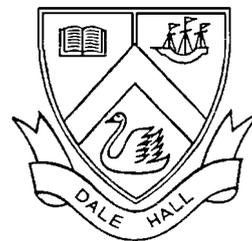
### **13.How will complaints regarding Online Safety be handled?**

The school will take all reasonable precautions to ensure Online Safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access. Any complaint about staff misuse is referred to the Headteacher. Complaints of cyberbullying will be dealt with in accordance with the school's anti-bullying policy. Complaints related to child protection will be dealt with in accordance with the school's and Local Authority child protection procedures.

### **14.Parental Support**

Parents' attention is drawn to the school Acceptable Use/Online Safety Policy in induction packs and on the school website. To safe guard the children, parents are required to sign and return the Home School Agreement. Parents are also required to discuss the Home School

**DALE HALL COMMUNITY PRIMARY SCHOOL  
ICT ACCEPTABLE USE/ONLINE SAFETY POLICY**

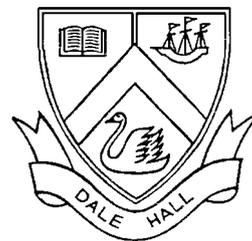


Agreement with their child and ask their child to sign and return it too. Both agreements need to be returned to school before their child is allowed access to the internet in school.

**15. Document History**

Date	Description
9 June 2015	Adopted by the Learning and Achievement Committee
20 November 2018	Rewrite by the ICT Leader with input from the children Added Safeguarding statement

# DALE HALL COMMUNITY PRIMARY SCHOOL ICT ACCEPTABLE USE/ONLINE SAFETY POLICY

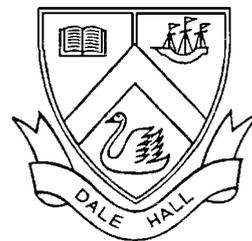


## Appendix 1: With Children

Staff need to:

- make pupils aware of appropriate behaviours when using the Internet
- remind children of the rules for using the Internet, including social media use and inform them of who to go to if they are uncomfortable with what they have seen or been made aware of online
- watch for accidental access to inappropriate materials and report the offending site to the Headteacher. If undesirable material is discovered, switch off the monitor, not the computer.
- check before publishing children's work on the school web site to make sure that the school has parental permission
- report any breaches of this policy to the Head Teacher
- ensure safe use of e-mail
- ensure safe use of school network, equipment and data
- ensure safe use of digital images and digital technologies, such as mobile phones, phone and digital cameras
- be aware that e Bullying / Cyberbullying can take place out of school
- be aware of their role in providing e-Safety education for pupils
- be aware that e-mail addresses are created for a whole class or teaching groups, not for individuals
- immediately report any illegal, inappropriate or harmful material or incident, they become aware of, to the appropriate person.

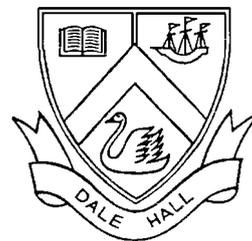
# DALE HALL COMMUNITY PRIMARY SCHOOL ICT ACCEPTABLE USE/ONLINE SAFETY POLICY



## **Appendix 2: Personal use by Staff**

- Internet access in all schools is filtered to prevent the viewing and downloading of inappropriate material. Do not attempt to access inappropriate sites. Downloading some material is illegal and the police or other authorities may be called to investigate such use.
- Only use chat and social networking sites responsibly and will keep online profiles professional. Staff will not engage in any on-line activity that may compromise their professional responsibilities.
- Staff will inform the school if they are accessing the school's Wi-fi on a personal device.
- Use of school Internet access for social media (other than school Facebook page), business, profit, advertising, or political purposes is strictly forbidden
- Only communicate with students / pupils and parents / carers using school email address. Any such communication will be professional in tone and manner.
- Be professional in all communications and actions when using school ICT systems.
- Please respect other people's material and do not corrupt, interfere with or destroy them. Do not open other people's files without express permission.
- Do not give details of usernames or passwords to anyone. Always remember to log out and close the browser when finished. Staff are to inform the Headteacher if someone else is thought to be using or be aware of their password.
- Do not release or in any way make available personal details of any colleague or pupil (phone numbers, fax numbers or personal e-mail addresses) over the Internet.
- When working with SIMS or any other personal data ensure that the data is secure.
- Do not take digital photographs or videos using personal digital cameras or mobile phone cameras

# DALE HALL COMMUNITY PRIMARY SCHOOL ICT ACCEPTABLE USE/ONLINE SAFETY POLICY



## **Appendix 3: Network Etiquette and Privacy**

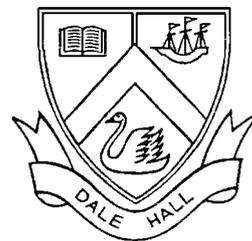
Users are expected to abide by the rules of network etiquette. These rules include, but are not limited to, the following:

- Be polite – never send or encourage others to send abusive messages that are likely to cause annoyance, inconvenience or needless anxiety.
- Use appropriate language – users should remember that they are representatives of the school on a global public system. Illegal activities of any kind are strictly forbidden.
- Do not use language that could be calculated to incite hatred against any ethnic, religious or other minority group.
- Make sure nothing in the messages could be interpreted as libellous.
- Privacy – do not reveal any personal information (e.g. home address, telephone number) about yourself or other users. Do not trespass into other users files or folders.
- Electronic mail – Is not guaranteed to be private. Messages relating to or in support of illegal activities will be reported to the authorities. Do not send anonymous messages.
- Do not send any unsolicited promotional or advertising material nor any chain letters or pyramid selling schemes.
- Disruptions – do not use the network in any way that would disrupt use of the network by others.
- Pupils will not be allowed access to unsupervised and/or unauthorised chat rooms and should not attempt to gain access to them.
- Do not attempt to visit websites that might be considered inappropriate.
- It is the responsibility of the User (where appropriate) to take all reasonable steps to ensure compliance with the conditions set out in this Policy document, and to ensure that unacceptable use of the Internet/Intranet does not occur.

## **Appendix 4: Examples of Unacceptable Use**

- Accessing or creating, transmitting, displaying or publishing any material e.g. images, sounds or data that is likely to cause offence, inconvenience or needless anxiety.
- Accessing or creating, transmitting or publishing any defamatory material.
- Receiving, sending or publishing material that violates copyright law. This includes through Video Conferencing and Web Broadcasting

## DALE HALL COMMUNITY PRIMARY SCHOOL ICT ACCEPTABLE USE/ONLINE SAFETY POLICY

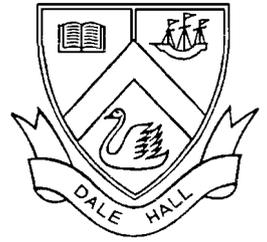


- Receiving, sending or publishing material that violates Data Protection Act or breaching the security this act requires for personal data. Transmitting unsolicited material to other users (including those on other networks).
- Unauthorised access to data and resources on the school network system or other systems.
- User action that would cause corruption or destruction of other users' data, or violate the privacy of other users, or intentionally waste time or resources on the network or elsewhere.
- Any use of the network that would bring the name of the school into disrepute is not allowed.

### **Appendix 5: Pupil Online Rules**

- I will always make sure a responsible adult is aware when we are online on any device and have permission to go on the websites I am using.
- I will not communicate (e.g. talk, video, email) online in anyway with people we do not know and we will tell an adult before we communicate with anyone, even people we do know.
- I will *not give out my or anyone else's personal information such as name, phone number or home address to anybody or wear school uniform on social media*. I will not arrange to meet anyone I may encounter online.
- I will not tell other people my ICT passwords.
- I will not deliberately look for, save or send anything inappropriate (things that are unpleasant, nasty, not age appropriate or that I know my parents or teacher would not approve of). If I accidentally find anything like this I will tell my teacher or a trusted adult, immediately.
- If we receive anything (like emails, chain messages, messages, pop ups or images) that we don't like we will tell a responsible adult and together we can decide whether it needs reporting.
- I will only use ICT in school for school purposes.
- When we have class emails or school email addresses I will only use them when e-mailing. I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- I will only open e-mail attachments from people I know, or people my teacher has approved.
- I will only open/delete my own files.
- I will be responsible for my behaviour when using ICT because I know that these rules are beneficial to my online welfare and to keep me safe.
- I will listen to the advice given by the school.
- I will not deliberately upload or add any images, video, sounds or text that could upset any member of the school community.
- I know that my use of ICT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my online safety.
- I will not join any social media sites if I am under the age limit.

**DALE HALL COMMUNITY PRIMARY SCHOOL  
ICT ACCEPTABLE USE/ONLINE SAFETY POLICY**



- I will ask my parent or carer for permission and help if I want to download something.
- I will follow this agreement in and out of school.

I have read, understood and agree with the terms in the ICT acceptable use/Online safety policy

Name \_\_\_\_\_

Sign \_\_\_\_\_

Date \_\_\_\_\_