



ASHGATE PRIMARY SCHOOL

Acceptable use of ICT and E Safety Policy

Ashgate Primary School, Ashbourne Road,
Derby DE22 3FS
Telephone 01332 343928
Email:- Admin@ashgate.derby.sch.uk

Supporting Documents:

- Practices for Storage of Safeguarding Files
- School Computing Policy
- Social Networking Policy (Staff)
- School Handbook

Head teacher: Mr Peter Sargent

Overview

ICT encompasses all computer based and internet technologies and electronic communications such as computers, mobile devices (ipads) as well as collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

Our ICT Acceptable Use and E Safety Policy has been written by the school, building on the DCC and DFS guidance.

The school's e-safety elements operate in conjunction with other policies including those for Computing, Acceptable Behaviour, Anti-bullying, Curriculum, Safeguarding, Data Protection and Security Procedures.

The role of coordinating e-safety matters will be the responsibility of the Designated Safeguarding Lead, the governor responsible for safeguarding and supported by the Computing Coordinator.

Expecations

Ashgate Primary School expects that all staff and pupils will:

- behave at all times within the terms of current legislation and the expectations of the school community;
- only use school ICT resources to further curriculum, professional and managerial responsibilities or other uses that are sanctioned by the head teacher or governors;
- make careful and considerate use of the schools ICT resources, report faults and work in a way that minimises the risk of introducing computer viruses to the system.
- protect everyone in school from the harmful or inappropriate material accessible via the Internet or transportable on computer media;
- help children to use email and similar systems appropriately and anonymously;
- recognise their responsibility to maintain the privacy of individuals;
- know and abide by the schools acceptable use policy as it applies to them and to the people in their care.
-

Appropriate Use

The school's ICT resources are to be used to enhance learning and teaching and are not for private and/or personal use, unless the school's Headteacher has given specific permission.

Internet and Email Access

Published content and the school web site

The school will only publish its own address, e-mail and telephone number on the school website. Staff and pupils' personal information will never be published on the school's website.

The school's head teacher will take overall editorial responsibility and ensure that content is both accurate and appropriate at all times.

Publishing pupil's images and work

Written permission from parents or carers will be obtained before photographs of pupils will be published on the school Web site.

Once a consent form has been signed and returned, parents still retain the right to withdraw consent at any stage, but they need to do so in writing.

Pupils' full names will not be used anywhere on the Web site or on any Blog or podcast. In addition, any photographed children will never be named.

As with photographs, pupil's work will only be published once the school has the permission of the pupil and parents. This permission will be sought annually although parents can amend their views during the academic year. The school will ensure that pupil's work is not published to the Internet until it has received written permission from the parent or guardian.

Safe access to the Internet

At Ashgate Primary School we aim to keep our children safe when using the Internet. The school's Internet Service Provider (ISP) has a stringent filtering system in place so that children are protected whilst using the Internet.

If staff or pupils discover an unsuitable site, they will turn off the monitor and report the site to the ICT co-ordinator or member of the Senior Leadership Team.

Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Social networking sites

The school's Internet Service provider has blocked all social networking sites so children are unable to access them at school (see above).

In addition, we teach our children to never to give out personal details of any kind which may identify them or their location.

The school has a specific Social Networking Policy.

E-mail

Pupils may only use approved e-mail accounts on the school system.

Pupils must immediately tell a teacher if they receive offensive e-mail.

Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.

E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.

Virus Protection

The school uses antivirus software. This software ensures that all networked machines are kept up to date against viruses. This ensures that children and staff are protected from malicious spyware or pop up windows which might contain inappropriate material.

Legal Issues

- All of the school's software is legally licensed and catalogued.
- No software can be added to machines unless permission has been given by the school's ICT coordinator.
- No materials generated in school about pupils is to be shared (either via e-mail or via the school's website) unless the author has been given authorisation to share such information or it has been checked and approved by a member of the Senior Leadership Team.

Security of ICT Resources

Ashgate Primary School has clear security measures to help protect its ICT equipment.

- A full audit of ICT equipment will be completed annually.
- The school has security etched all equipment with 'Selectamark'. Selectamark stickers are clearly attached to help to deter thieves.
- The ICT storage equipment is locked up every night before the school is closed.
- Laptops are never left on display over night, they are either taken home by the class teacher or placed in a secure room/lap safe.

Data Protection at Ashgate Primary School

All members of the school community can save appropriate material onto the school network. The staff area can only be accessed by staff who each have an individual password to ensure

that children cannot access any staff material.

Informal checks ensure that only appropriate material is stored on the school's server.

Password Protocol

Every member of staff and all of the children are given a unique user name and password to access the school network. User names and passwords are individual and people are required not to share this information with others. School staff also may have access to the Derby City Portol website and the assessment data such as Otrack; for these staff have a unique user name and they are able to change their own password.

To be in line with the Computer Misuse Act 1990, all users must only use their own user name and password and must not share this information with others. If users are required to access programs within school systems, they must access them using their own logon. If this is not possible, they must ensure they obtain appropriate access by asking the headteacher/school administrator to make arrangements for them to obtain access to all required areas using their own logon.

Privacy

The school will collect personal information about you fairly and will let you know how the school and Derby LA will use it. The school will use information about pupils to further curriculum, professional and managerial activities in accordance with the business of the school and will contact the parents or guardians, if it is necessary, to pass information beyond the school or Derbyshire LA. For other members of the community the school will tell you in advance if it is necessary to pass the information on to anyone else other than the school and Derby LA.

The school will hold personal information on its systems for as long as you remain a member of the school community and remove it in the event of your leaving or until it is no longer required for the legitimate function of the school. We will ensure that all personal information supplied is held securely, in accordance with the policies and practices of Derby City Council and as defined by the Data Protection Act 1998.

You have the right to view the personal information that the school holds about you and to have any inaccuracies corrected.

Disposal of ICT Resources

Ashgate Primary School will dispose of any ICT resources in line with current DCC protocol.

Therefore Governor approval will be sought before ICT resources are disposed. Following Governor approval, all equipment which contains sensitive files will have their hard disk drives wiped, and serial numbers will be collected. Finally, the Ashgate Primary School's ICT hardware audit will be updated as well as the school's inventory.

Backing Up Procedures

Administration System

- The school ICT technician ensure that an automated systematic back up of data is completed on a regular basis so that recovery of essential data can be managed in the event of loss of data files or system failure.
- An electronic and/or paper based record of all back ups will ensure the most up to date

information is retrieved. Backups are automatically time/date stamped.

Curriculum System

Ashgate Primary School's work is backed up daily and weekly. This means that both staff and children's work is protected every week.

Wider E Safety and the reporting of incidents

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. Neither the school nor DCC can accept liability for the material accessed, or any consequences of Internet access.

The school will audit ICT provision to establish if the e-safety policy is adequate and that its implementation is effective. Designated Safeguarding Lead and Governor to audit the safety and security of school computer systems in conjunction with DCC technician.

The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

Handling e-safety complaints:

Complaints of Internet misuse will be dealt with by a senior member of staff.

Any complaint about staff misuse must be referred to the head teacher.

Complaints of a Safeguarding nature must be dealt with in accordance with school Safeguarding procedures.

Parents and children will need to work in partnership with staff to resolve issues. Issues not resolved will be taken through the appropriate disciplinary procedures.

Reporting

All breaches of the e-safety policy need to be recorded in the ICT reporting book that is kept in the general office. The details of the user, date and incident should be reported. Incidents, which may lead to child protection issues, need to be passed on to the Designated teacher immediately – it is their responsibility to decide on appropriate action not the class teachers.

Incidents, which are not child protection issues but may require SLT intervention, (eg cyberbullying) should be reported to SLT in the same day.

Allegations involving staff should be reported to the head teacher. If the allegation is one of abuse then it should be handled according to the DFE document titled 'Dealing with allegations of abuse against teachers and other staff'. If necessary the local authority's LADO should be informed.

Evidence of incidents must be preserved and retained.

The curriculum will cover how pupils should report incidents (eg Ceop button, trusted adult, Childline)

Infringements and sanctions

Whenever a student or staff member infringes the e-Safety Policy, the final decision on the level of sanction will be at the discretion of the school management.

The following are provided as exemplification only:

(a) Students

Level 1 infringements

- Use of non-educational sites during lessons
- Unauthorised use of email
- Unauthorised use of mobile phone (or other new technologies) in lessons e.g. to send texts to friends
- Use of unauthorised instant messaging / social networking sites

[Possible Sanctions: referred to class teacher / e-Safety Coordinator/ confiscation of phone]

Level 2 infringements

- Continued use of non-educational sites during lessons after being warned
- Continued unauthorised use of email after being warned
- Continued unauthorised use of mobile phone (or other new technologies) after being warned
- Continued use of unauthorised instant messaging / social networking sites
- Use of Filesharing software
- Accidentally corrupting or destroying others' data without notifying a member of staff of it
- Accidentally accessing offensive material and not notifying a member of staff of it

[Possible Sanctions: referred to Class teacher / e-safety Coordinator / Headteacher / removal of Internet rights for a period / contact with parents]

Level 3 infringements

- Deliberately corrupting or destroying someone's data, violating privacy of others

- Sending an email or message that is regarded as harassment or of a bullying nature (one-off)
- Deliberately trying to access offensive or pornographic material

[Possible Sanctions: referred to Class teacher / e-safety Coordinator / Headteacher / removal of Internet rights for a period / contact with parents]

Other safeguarding actions

If inappropriate web material is accessed:

1. Ensure appropriate technical support filters the site
2. Inform SSCB/LA as appropriate

Level 4 infringements

- Continued sending of emails or messages regarded as harassment or of a bullying nature after being warned
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988
- Bringing the school name into disrepute

[Possible Sanctions – Referred to Head Teacher / Contact with parents / possible exclusion / refer to Community Police Officer / LA e-safety officer]

Other safeguarding actions:

1. Secure and preserve any evidence
2. Inform the sender's e-mail service provider if a system other than the school system is used.

Pupils are also informed that sanctions can be applied to e-safety incidents that take place out of school if they are related to school.

(b) Staff

Level 1 infringements (Misconduct)

- Excessive use of Internet for personal activities not related to professional development e.g. online shopping, personal email, instant messaging etc.
- Misuse of first level data security, e.g. wrongful use of passwords
- Breaching copyright or license e.g. installing unlicensed software on network

[Sanction - Headteacher. Warning given.]

Level 2 infringements (Gross Misconduct)

- Serious misuse of, or deliberate damage to, any school / Council computer hardware or software;
- Any deliberate attempt to breach data protection or computer security rules;
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent;
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988;

- Bringing the school name into disrepute.

[Sanction – Referred to Headteacher / Governors and follow school disciplinary procedures; report to LA Personnel/ Human resources, report to Police.

Other safeguarding actions:

1. Remove the PC to a secure place to ensure that there is no further access to the PC or laptop.
2. Instigate an audit of all ICT equipment by an outside agency, such as the schools ICT service providers - to ensure there is no risk of pupils accessing inappropriate materials in the school.
3. Identify the precise details of the material.

If a member of staff commits an exceptionally serious act of gross misconduct they should be instantly suspended. Normally though, there will be an investigation before disciplinary action is taken for any alleged offence. As part of that the member of staff will be asked to explain their actions and these will be considered before any disciplinary action is taken.

Schools are likely to involve external support agencies as part of these investigations e.g. an ICT technical support service to investigate equipment and data evidence, the Local Authority Human Resources team.

Rewards

Whilst recognising the need for sanctions it is important to balance these with rewards for positive reinforcement. The rewards can take a variety of forms – eg. class commendation for good research skills, certificates for being good cyber citizens etc. Each year group co-ordinator will indicate these opportunities within the provided planning.

Ashgate Primary School – Acceptable use of ICT Agreement

All pupils use computer facilities including Internet access as an essential part of learning, as required by the National Curriculum. Both pupils and their parents/carers are asked to sign below to show that our ICT Safety rules have been understood and agreed. By admitting your child to Ashgate Primary School, you are agreeing to the following statements

Pupil Agreement:

- I will ask permission before using the internet.
- I will only use websites that an adult has chosen.
- I will immediately tell an adult, and turn off my monitor, if I see any webpage I am uncomfortable with.
- I will only e-mail people an adult has approved and write them in a polite and friendly manner.
- I will never give out personal information or passwords.
- I will not open e-mails sent by anyone I don't know.
- I will not use chat rooms or social networking sites unless a specific use is approved.
- I will not bring in computer games or files from home unless asked by a teacher.

Parent/Guardian Agreement:

- The school has installed ICT equipment (computers which are connected to the internet) to help with your child's learning. The Internet Service Provider used by this school provides a continually updated, filtered service to attempt to ensure only acceptable Internet sites are available.
- Your child's teacher will only set ICT work which is related to the curriculum and which will benefit their learning.
- We encourage you to contact the school if you have any concerns regarding your child's use of our ICT provision, and our 'Acceptable Use Policy' is available for viewing in our office.
- Portable storage devices (DVD's, Memory Sticks etc) from home, cannot be used in school due to virus and licensing implications.
- Occasionally digital images containing children and/or their work will be taken. Permission will be sought before these are stored or used in school. The computers in school can only be accessed through username and password.
- Our school website may occasionally have children's work, or images of them working, but children will not be named.

In addition staff:

- Supervise children using the internet at all times.
- Check that the sites pre-selected for pupil use are appropriate to the age and maturity of pupils.
- Are extra vigilant when pupils are undertaking their own research and check that pupils are following the agreed search plan.