CHARLESWORTH SCHOOL

...from tiny acorns great oaks grow

e-safety Policy

Purpose:

The development and expansion of the use of ICT, and particularly of the internet, has transformed learning in schools in recent years. Children will need to develop high level ICT skills, not only to maximise their potential use as a learning tool, but also to prepare themselves as lifelong learners and for future employment. Schools have made a significant investment both financially and physically to ensure these technologies are available to all learners.

New technologies have become integral to the lives of children 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 students learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children should have an entitlement to safe internet access at all times.

The requirement to ensure that children 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 use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil / student achievement.

However, the use of these new technologies can put children 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 child.

Many of these risks reflect situations in the off-line world and it is essential this e-safety policy will be used in conjunction with other Charlesworth School policies (eg behaviour, anti-bullying and child protection policies).

Schools must, through their e-safety policy, ensure that they meet their statutory obligations to ensure that children are safe and are protected from potential harm, both within and outside school. As with all other risks, it is impossible to eliminate those completely from our children's lives. It is therefore essential, through our good educational provision to build students' / 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.

At Charlesworth School we aim to demonstrate that we can provide the necessary safeguards to help ensure that we have done everything we can 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 children (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.

Aims and Objectives:

This policy is designed to protect the children at Charlesworth School from safeguarding issues that may arise due to the use of the internet and other technologies. It applies to all members of the school community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.

The Education and Inspections Act 2006 empowers Head teachers, to such extent as is reasonable, to regulate the behaviour of students / 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:

Head teacher and Senior Leader:
The Head teacher is responsible for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be by the E-safety co-ordinator and will be an issue for all members of the school community.

- The Head teacher / Senior Leadership team are responsible for ensuring that all staff receive suitable CPD to enable them to carry out their e-safety roles within their classes/ roles.
- The Head teacher/ Senior Management Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of the school community.

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 Head teacher/ E-safety coordinator for investigation / action / sanction

- e-safety issues are embedded in all aspects of the curriculum and other school activities
- children understand and follow the school e-safety and acceptable use policy
- children 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 students / 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.

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 Sarah Smith as ICT Governor and Russell Lear as the Chair of Governors, who will receive regular information about e-safety incidents and monitoring reports.

E-Safety/ ICT Coordinator:

It is strongly recommended that each school should have a named member of staff with a day to day responsibility for e-safety. At Charlesworth School this role will be linked to ICT coordination and the lead for ICT within the school. It will be the responsibility of the e-safety co-ordinator to:

- Take the day to day responsibility for e-safety issues and have a leading role in establishing and reviewing the school e-safety policies / documents
- Ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- Provide training and advice for staff
- Liaise with the Local Authority
- Liaise with school ICT technical staff
- Receive reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- Meet regularly with members of the Governing body to discuss current issues, review incident logs and filtering / change control logs
- Attend relevant meeting / committee of Governors
- Report regularly to the Senior Leadership Team

Network Manager:

The outsourced IT company (currently Sasaage) are responsible for ensuring that:

- The school's ICT infrastructure is secure and is not open to misuse or malicious attack.
- The school meets the e-safety technical requirements
- Users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed

- That users 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 monitoring software / systems are implemented and updated as agreed in school policies

Pupils:

- Are responsible for using the school ICT systems in accordance with the Student / Pupil 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. At Charlesworth School we will therefore take every opportunity to help parents understand these issues through parents' meetings, newsletters, website and information about national / local e-safety campaigns. Parents and carers will be responsible for:

- endorsing (by signature) the Student / Pupil Acceptable Use Policy
- ensuring their children have an understanding of how to keep safe on the internet.
- monitoring their child's use of the internet and other technologies

Practice and Procedures:

Whilst regulation and technical solutions are very important, their use must be balanced by educating our children to take a responsible approach. The education of children in e-safety is therefore an essential part of Charlesworth School's e-safety provision. Children need the help and support from 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 is taught within ICT, PSHE and other lessons and is revisited every term in each class from Reception to Year 6 - this covers both the use of ICT and new technologies in school and outside school
- Key e-safety messages will be reinforced as part assemblies and pastoral activities.
- Children will be taught within lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information

- Children will be helped to understand the need for the student 'Acceptable Use Policy' and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- All Staff will act as good role models in their use of ICT, the internet and mobile devices

Education – parents / carers:
Some parents and carers may 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 come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. At Charlesworth School we will therefore seek to provide information and awareness to parents and carers through newsletters, the school website and parents meetings.

Education & Training – Staff:
It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training should support staff's CPD and needs to be offered on a regular basis as needs are identified.

- E-safety training will be made available to staff through staff meetings/ INSET days. An audit of the e-safety training needs of all staff will be carried out regularly. Some staff may identify e-safety as a training need within the performance management process and this need must be addressed fully.
- 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 E-Safety Coordinator will receive regular updates through relevant LA courses and by accessing guidance by CEOP or other relevant organisations.
- This E-Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The E-Safety Coordinator will provide advice / guidance / training as required to individuals as required

Training – Governors:
Nominated Governors should take part in e-safety training / awareness sessions. This may be offered through either LA run training sessions or by participation in school training/ information sessions for staff or parents

Technical – infrastructure / equipment, filtering and monitoring:
As a School we 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 e-safety responsibilities:

- School ICT systems will be managed in ways that ensure that the school meets the e-safety technical requirements.
- 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 children in Key Stage 2 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.
- Children in Foundation Stage/ Key Stage 1 will have class log-on's and passwords in order to access the school computers.
- The "master / administrator" passwords for the school ICT system, used by the Network Manager/ ICT technician must also be available to the Head teacher and Senior leader and kept in a secure place.
- All 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 has provided enhanced user-level filtering through the use of the EMBC filtering programme.
- Any filtering issues should be reported immediately to EMBC.
- Requests from staff for sites to be removed from the filtered list will be considered by the Head teacher and Network Manager (Complink). If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly.
- 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. •
- Appropriate security measures are in place to protect the servers, firewalls, routers, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.
- 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.

Curriculum:

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

- in lessons where internet use is pre-planned, it is best practice that children 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 children 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 Head teacher/ Network Manager (Complink) can 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.
- Children 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

Use of digital and video images - Photographic, Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and children instant use of images that they have recorded themselves or downloaded from the internet. However, staff and children 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.

- When using digital images, staff should inform and educate children about the risks associated with the taking, use, sharing, publication and distribution of images.
- 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.
- Care should be taken when taking digital / video images that children are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Children must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, Learning platform or elsewhere that include children will be selected carefully and will comply with good practice guidance on the use of such images.
- Children's 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 children are published on the school website. This will be obtained through the Parents Acceptable Use Policy.
- Children's work can only be published with the permission of the student / 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.

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 :

The use of mobile phones by children is strictly forbidden within the school environment. Children will need to hand their mobile phones to their class teacher for safe keeping if brought to school.

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.
- Users must immediately report, to head teacher 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 students / pupils or parents / carers (email, chat, Learning Platform etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems.
- Whole class or group email addresses will be used at KS1, while children at KS2 and above will be provided with individual school email addresses for educational use.
- Children 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 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 certain internet usage as follows:

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. If any incidents of this nature occur they must be directly referred to the Head teacher.

Monitoring and Review

The Headteacher and Governing Body will review the implementation of the e-Safety Policy in line with the agreed schedule for policy review.

Staff and governors will be involved and asked to contribute to the review and all staff will be informed of the outcome of the review.

e-Safety Policy

Charlesworth School

	Date	**Minute No.**
Approved by Governors	_____	_____
Reviewed by Governors	_____	_____
Reviewed by Governors	_____	_____
Reviewed by Governors	_____	_____
Reviewed by Governors	_____	_____
Reviewed by Governors	_____	_____
Reviewed by Governors	_____	_____
Reviewed by Governors	_____	_____
Reviewed by Governors	_____	_____
Reviewed by Governors	_____	_____
Reviewed by Governors	_____	_____
Reviewed by Governors	_____	_____
Reviewed by Governors	_____	_____
Reviewed by Governors	_____	_____

Staff Signature Sheet		
Name	**Signature**	**Date**