Dunholme St Chad's
Church of England Primary School

e-Safety Policy

Policy Information			
Status:	Non-statutory	**Reviewed by:**	School (seen by Governors on request)
Cycle Review:	In line with current practice	**Policy approved:**	July 2017
Approved by:	Carl Parkin (IT Lead)	**Signature:**	

Dunholme St Chad's Church of England Primary School
e-Safety Policy

The Internet is part of the statutory curriculum and an entitlement for pupils. It is used at Dunholme St. Chad's to raise educational standards and promote pupils achievements. All people working in this school whether adult or child have a duty to be aware of e-safety at all times, to know the required procedures and to act on them. The school will take all reasonable precautions to ensure that users access only appropriate material, however, due to the global and connected nature of internet, content it is not always possible to guarantee that access to unsuitable material will never occur in school.

1. Our vision, values and aims

Our vision
We aspire to be a school, which families actively choose knowing their children will be happy and listened to. Our children will enjoy an inspirational curriculum and exceptional teaching which empowers learning.

Our values
St. Chad's example of love, truth and humility underpins all that we do and from which we promote the values of respect, co-operation, empathy, responsibility, honesty, tolerance, understanding and trust.

Our aims
We aim to provide a broad, balanced and creative curriculum which will enable all pupils to become successful learners, confident individuals and responsible citizens.

2. 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 receiving regular information about e-safety incidents and monitoring reports. Esther Watt-Jones, a member of the Governing Body is E-Safety Governor.

The role of the e-Safety Governor will include:

- regular reviews with the e-Safety Co-ordinator,
- regular monitoring of e-safety incident logs;
- reporting to relevant Governors meeting,

Headteacher and Senior Leaders
The Headteacher and senior leaders are responsible for ensuring:

- the safety (including e-safety) of members of the school community along with the E-safety coordinator,
- that the e-Safety Coordinator and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant,
- 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.

When issues arise regarding safeguarding issues, teachers will notify Dunholme St Chad's designated lead Patricia Ruff, and in her absence Sara Bristow, and when appropriate they will notify the LA.

The Headteacher and another member of the Senior Leadership 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 staff.

E-Safety Coordinator

E-Safety Coordinator (Carl Parkin):

- 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 technical staff,
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments,
- reports regularly to Senior Leadership Team.
    - Records incidents related to E-Safety and reports to parents about the issues and sanctions put in place.

Incidents will be dealt with and the investigation / action / sanctions will be the responsibility of the E-Safety Co-ordinator unless the incident relates to allegations against staff in which case LA procedures will be followed.

Teachers and Support Staff

Teachers 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 and understood the school Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to the e-Safety Co-ordinator /Headteacher / Senior Leader / ICT Co-ordinator / Class teacher / (as in the section above) for investigation / action / sanction,
- digital communications with pupils (email / blogging) 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.

Designated person for Safeguarding

The designated person for Safeguarding 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.

Pupils
- 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:
- accessing the school website / blogging in accordance with the relevant school Acceptable Use Policy.

Community Users
Community Users who access school ICT systems / website as part of the Extended School provision will be expected to conform to the AUP.

3. Internet access

- Staff and children must not access or attempt to access any sites that contain any of the following: child abuse; pornography; promoting discrimination of any kind; promoting racial or religious hatred; promoting illegal acts; any other information which may be illegal or offensive to colleagues.
- It is recognised that inadvertent access may happen. Should staff or a pupil access any of these sites unintentionally staff should report the matter to the Head Teacher, or in her absence, the Assistant Headteacher, so that it can be logged.
- The Headteacher (or in her absence, the Assistant Headteacher) has a responsibility to report any of the following to Lincolnshire Police:
  - images of child abuse (sometimes incorrectly referred to as child pornography). These are images of children apparently under 16 years old involved in sexual activity or posed to be sexually provocative;
  - adult material that potentially breaches the Obscene Publications Act;
  - criminally racist material in the UK.

4. Social Networking Sites

Access is not allowed in school. Staff receive education in the dangers of Social Networking sites and appropriate guidance in their use as part of their induction process. Children receive education in the dangers of Social Networking sites and appropriate guidance in their use through the PSHE and Safeguarding curriculum.

Staff should fully acquaint themselves with the privacy settings that are available on any social networking profile in order that profiles are not publicly available.

Members of staff (Teachers, Teaching Assistants and all support staff) should never knowingly become 'friends' with pupils on any social networking site or engage with pupils on internet chat. Likewise they should never knowingly become 'friends' with former pupils until they are sure that the former pupil is mature enough to accept the responsibility of the 'friendship', i.e. over the age of 18 years.

All staff should be aware of the potential dangers of social networking sites. Anything that is published online has the potential to be seen by pupils, parents and colleagues. Before you post images, information or comments, consider whether it could be misconstrued by anyone or has the potential to cause damage to the reputation of the profession, the school or yourself.

The school's confidentiality policy must be adhered to at all times.

Children will receive appropriate curriculum and e-safety lessons that will teach about the dangers of social networking linked to ideas about cyber-bullying.

5. Use of Email

All members of staff should use their professional e-mail address for conducting school business. Use of school e-mail for personal/social use should be used with caution.

6. Passwords

Passwords are confidential and individualised to each person. On no account should a member of staff allow a pupil to use a staff login.

Children should also only use their own passwords and never trespass on folders and files that do not belong to them when working on shared access drives.

7. Cyber-Bulling

All staff with ensure that lessons throughout the school year as part of the computing and PSHE curriculum will tackle issues such as cyber-bullying and make children aware to appropriate actions to take when working with technology.

Any incidents of cyber-bullying will be recorded, as per the anti-bullying procedures, and appropriate level of intervention and sanctions put into place.

8. Data Protection

Where a member of staff has to take home sensitive or confidential information sufficient safeguards should be in place to prevent loss or misuse, i.e. is it really necessary to take it all home, can it be encrypted, does it have to be on a USB memory stick which can be easily misplaced?

9. File sharing

Technology such as peer to peer (P2P) and bit torrents are not permitted on the Lincolnshire School's Network.

10. Personal Use:

Staff are not permitted to use ICT equipment for personal use without prior permission from the Headteacher. The school emphasises that all use should be within the boundaries of acceptance, and have due regard to the replacement and maintenance cost of ICT equipment. Staff should also be aware that ICT equipment may be subject to monitoring checks.

11. Images and Videos:

Staff and pupils should not upload onto any internet site, images or videos of themselves or other staff or pupils without consent.

Videos and images of children should only be used on the school website and not including any children who do not have permission from a parent to be on there.

12. Use of Personal ICT:

Use of personal ICT equipment is at the discretion of the headteacher. Any such use should be stringently checked for up to date anti-virus and malware checkers.

13. Viruses and other malware:

Any virus outbreaks are to be reported to the Service Provider as soon as it is practical to do so, along with the name of the virus (if known).

Staff should note that internet and email may be subject to monitoring

All Staff are required to sign a declaration annually to confirm that they have read and understood this Policy.

Breaches of this policy may be subject to the school's discipline procedures.

Appendix

E-safety and Acceptable User Policy (Staff)

- I have read and fully understand the attached Primary School e-safety and Acceptable User Policy which was prepared using the e-safety policy of Lincolnshire Safeguarding Children's Board and the Acceptable Use of ICT Policy (AUP).

- I understand that any breach of this policy may subject me to the school's disciplinary procedure.

- I am also aware that internet use and emails may be subject to monitoring.

SIGNED

DATED