Review Date February 2027

BELMONT CP SCHOOL

e-SAFETY POLICY

1 Introduction

This e-Safety Policy will be used in conjunction with policies/protocols including those for safeguarding, Acceptable Use of ICT, X, positive behaviour, curriculum and home-school agreement.

The Headteacher will act as the e-Safety Officer in relation to his role as Designated Safeguarding Lead (it is not a technical role). An additional member of staff has been appointed as a second e-Safety Officer. In conjunction with the ICT technician they will monitor the use of the internet and other digital technologies used in the school.

Our e-Safety Policy has been written by the school in accordance with government guidance and approved by the governing body.

2 Aims

The school aims to ensure that all pupils:

- Will use the internet and other digital technologies to support, extend and enhance their learning:
    - Pupils will be given clear objectives for internet use.
    - Web content will be subject to age-appropriate filters.
    - Internet use will be embedded in the curriculum.
- Will develop an understanding of the uses, importance and limitations of the internet and other digital technologies in the modern world including the need to avoid undesirable content and extremist or radical views or opinions as in line with the Prevent Duty. Pupils will be taught how to:
    - use the internet effectively for research purposes
    - evaluate information found on the internet
    - report inappropriate web content
- Will develop a positive attitude to the internet to enhance their learning experience through both independent and collaborative working.
- Will be taught e-safety to equip them with the knowledge to use existing, as well as up and coming, technologies safely.

3 Whole School Responsibilities

Headteacher

- Responsible for e-safety issues within the school but may delegate the day to day responsibility to the e-Safety Officer.
- Ensure that the e-Safety Officer is given time, support and authority to carry out their duties effectively.

- Ensure the e-Safety Officer is kept informed of development at Local Authority level.
- Ensure that the Governing body is kept informed of e-safety issues.
- Ensure that appropriate funding is allocated to support e-safety activities throughout the school.

e-Safety Officer

- Primary responsibility is to establish and maintain a safe ICT learning environment ensuring e-safety rules are displayed in school.
- In conjunction with the IT Co-ordinator to maintain a school-wide e-safety programme.
- Be responsible for ensuring staff are confident to delivery e-safety lessons to children and are aware of how to report incidents.
- Ensure the Acceptable Use of ICT Policy for staff and pupils (Appendix 1 and 2) is up to date.
- Monitor and review e-safety policies and procedures.
- Respond to e-safety incidents and record details in the e-safety incident log.
- Maintain a staff development programme relating to e-safety.
- Develop a parental awareness programme
- Ensure parents are kept up to date with e-safety concerns about gaming and social media which relate to activities outside of school.
- Maintain an understanding of relevant legislation.

Governing Body

- Appoint an e-safety governor.
- Support the Headteacher and e-Safety Officer in establishing and implementing policies, systems and procedures for ensuring a safe ICT learning environment.
- Promote e-safety to parents.

Technical Staff

- Provide a technical infrastructure to support e-safety practices.
- Ensure that appropriate processes and procedures are in place for responding to the discovery of illegal materials, or suspicion that such materials are, on the school's network.
- Ensure that appropriate processes and procedures are in place for responding to the discovery of inappropriate but legal materials on the school's network.
- Maintain an understanding of relevant legislation.
- Report network breaches of acceptable use of ICT facilities to the Headteacher and/or the e-Safety Officer.
- Maintain a professional level of conduct in their personal use of technology, both within and outside school.
- Take responsibility for their own professional development.

Teaching and Support Staff

- Contribute to the development of e-safety policies and procedures.
- Sign and adhere to the Staff Acceptable Use of ICT policy (Appendix 1) prior to using school IT equipment.
- Take responsibility for the security of data in accordance with the Data Protection Act and the Staff Acceptable Use of ICT policy.

- Model good practice in using new and emerging technologies.
- Maintain an awareness of e-safety issues, and how they relate to pupils in their care.
- Address e-safety concerns that arise as a result of gaming or social media, in or outside of school, and report these to the e-safety officer.
- Embed e-safety education in the delivery of the curriculum.
- Know when and how to escalate e-safety issues.
- Maintain a professional level of conduct in their personal use of technology, both within and outside school.
- Report any virus outbreaks to Infotechdirect and the e-Safety Officers who will, in turn, inform the relevant Local Authority Helpdesk as soon as it is practical to do so.
- Are aware that the school network and internet traffic is monitored, both at school and Lincolnshire County Council level and can be traced to an individual user. Discretion and professional conduct is essential at all times.

Pupils

- All pupils sign the Pupil Acceptable Use of ICT policy before access is granted to use school ICT equipment (Appendix 2).
- Pupils will be informed that network and Internet use will be monitored.
- Any deviation or misuse of ICT equipment or services will be reported to the e-Safety Officers.
- Pupil mobile phones are handed in at the school for safe keeping. Any necessary phone calls will be made by school staff.

Parents/Carers

Parents play the most important role in the development of their children; as such the school will ensure that parents have the skills and knowledge they need to ensure the safety of children outside the school environment.

- Through newsletters and the Belmont website the school will draw parents' attention to the school e-Safety Policy and keep them up to date with new and emerging e-safety risks.
- When appropriate, the school will inform parents of e-safety concerns regarding online gaming and social media and signpost parents to websites and articles which offer practical advice.

Parents must also understand the school needs to have rules in place to ensure that their child can be properly safeguarded.

- Parents will sign the Pupil Acceptable Use Policy before any access can be granted to their child to use school ICT equipment or services. They will also be made aware that all school Internet use is filtered and monitored.
- All parents must sign to confirm whether or not images, videos and names may be used for school purposes including the school website, X and local publications. Non-return of the permission slip will not be assumed as acceptance. Individual permission may be sought from parents if their child is attending an event outside school eg mini Olympics where photographs/video may be taken and used for promotional purposes.

Volunteers/Students

Any person not directly employed by the school will be asked to sign the Volunteer/Student Code of Conduct form before being allowed to access the internet from the school site.

4 ICT Activities

Data Protection - All sensitive or confidential information is stored/transferred with reference to the Data Protection Act and in accordance with the Staff Acceptable Use of ICT policy and the school Data Protection Policy.

Filtering - The school works with Infotechdirect and LCC to ensure systems to protect pupils are reviewed and improved. If staff or pupils come across unsuitable online materials, the site must be reported to the e-Safety Officers.

Social Networking

- The school will control access to social networking sites, and consider how to educate pupils in their safe use.
- Social networking sites such as Facebook, X, TikTok, Snapchat and WhatsApp are blocked by the ICT Technician. Pupils cannot log onto or search these sites in the school environment. However, YouTube may be used for educational purposes by staff.
- Should staff wish to use other social media sites, permission must first be sought via the e-Safety Officer who will advise the Headteacher for a decision to be made.
- Members of staff should never knowingly become 'friends' with pupils on any social networking site or engage with pupils on internet chat.
- Pupils will be advised never to give out personal details of any kind that may identify them, their friends or their location.
- Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.
- Pupils will be advised of the risks and told to strongly consider the use of nicknames and avatars if using social networking sites outside of school.

File Sharing - Technology such as peer to peer (P2P) and 'bit torrents' is not permitted on the Lincolnshire Schools' Network.

School Website - The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

- Staff or pupil personal contact information will not be published.
- Photographs/videos that include pupils will be selected carefully so that their image cannot be misused. Pupils' photographs/videos will only be used if parental consent has been given. Full names will not be used anywhere on the school website in association with photographs/videos.
- All uploaded data conforms to copyright law.
- If it should come to the school's attention that there is a resource that has been inadvertently uploaded, and the school does not have copyright permission to use that resource, it will be removed within one working day.

Parentmail – this method of communication is used to inform parents of school activities, closures etc.

- All parents and staff will be invited to register to receive electronic communication via Parentmail.
- Only authorised staff will have access to Parentmail.
- Parents' details will be deleted from Parentmail on request, or when their child(ren) leaves the school.

X - The Belmont CP School X account will be a public account which will run alongside more traditional methods of communication not replace them.

Microsoft Teams - This platform is used for remote learning and communication.

- All parents and staff are informed of the expectations of using Teams in line with our e-safety policy.
- All staff will follow safeguarding protocols when using video calls on Teams.
- All parents and children are informed that the chat and call functions must only be used for teacher/pupil communication and not for pupil/pupil communication.
- All staff, parents and children are informed that communication on Teams should directly relate to learning and be professional and courteous.

Managing Emerging Technologies

- Emerging technologies will be examined for educational benefit.
- A risk assessment will be made by the e-Safety Officer in liaison with the Infotechdirect Technical Staff and suitable control measures, for new technology, put in place.

Assessing risks

- e-Safety risk assessments will be implemented by the e-Safety Officer in liaison with Infotechdirect Technical Staff. Assessments will be monitored and reviewed regularly and when the need arises.
- The e-safety policy will be regularly reviewed to ensure that it is adequate, appropriate and effective.
- The school will take all reasonable precautions to prevent access to inappropriate 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 computer connected to the school network. Neither the school nor Lincolnshire County Council can accept liability for any material accessed, or any consequences of internet access.

Handling e-safety incidents

- All incidents alleging illegal or inappropriate activity will be dealt with in accordance with the school child protection procedures.
- All such incidents will be recorded on CPOMS.

Ratified by governors at their meeting held on	7 February 2024
Signed	
Review Date	February 2027

BELMONT CP SCHOOL
ACCEPTABLE USE OF ICT - STAFF

The purpose of this document is to minimise the risk to pupils of inappropriate contact from staff, to protect employees and the school from litigation and to minimise the risk to the school's ICT systems.

All users must take responsibility for their own use of new technologies, making sure that they use technology safely, responsibly and legally. All users must be active participants in e-safety education taking personal responsibility for their awareness of the opportunities and risks posed by new technologies and how they relate to pupils in their care.

In the event of any inappropriate or illegal activity staff should refer to the e-safety flowchart and also record the incident on CPOMS.

Minimising the Risk

- Staff working closely with children, especially on a 1:1 basis or assisting with personal care should ensure mobile phones are not kept on their person but are stored away securely in a designated location.
- Belmont school uses encryption software to ensure that all data is safely secured. All data must be stored onto the encrypted school system. Under no circumstances can memory sticks be used to store sensitive data temporarily.
- If memory sticks are used for storing non-sensitive data, they must be checked by the school office for viruses before being used on school equipment.
- Users are required to protect their password and not share their account details with others for their use, nor utilise another users' account or misrepresent their identity for any reason. Users must not under any circumstances reveal their password to anyone else.
- Passwords must be changed at least every six weeks.
- Users must ensure that they lock their equipment if they leave it unattended.
- No user shall access (eg read, write, modify, delete, copy, move) another user's personal electronic documents (including email) without the owner's permission or as allowed by this policy or by law. Any user caught trying to gain access to another user's accounts, files or data will be subject to disciplinary action.
- Users must ensure any software used has a valid licence. When installing apps, programmes or music users should use care so as not to violate Copyright.
- Users must ensure electronic resources are accessed and used within applicable Copyright requirements and usage is recorded as appropriate eg music, video, online articles (Appendix B)
- No one may use school ICT resources eg laptops, iPads etc to 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. Inadvertent access must be treated as an e-safety incident, reported to the e-Safety Officers and an incident sheet completed.
- No one may use school ICT resources to transmit abusive, threatening or harassing material, chain letters, spam or communications prohibited by law.
- Under normal circumstances no member of staff should engage in direct communication (in or out of school) of a personal nature with a pupil who is not a member of their own direct family,

by any means eg email, SMS text messaging. Should special circumstances arise where such communication is felt to be necessary, the agreement of Headteacher should be sought first and appropriate professional language should be used at all times.

- Accessing social networking sites (eg Facebook, X, Snapchat etc) and/or Ebay, during lessons/after school clubs is strictly prohibited. Careful consideration should also be given to content when using social networking sites outside school.
- Cameras/iPads provided by the school may be used to take photographs to support teaching and learning. They should not be used to take inappropriate, illicit or sexually explicit photographs or videos, nor should they be used to embarrass anyone in any way. The use of personal ICT equipment is at the discretion of the Headteacher eg mobile phone camera used on a school visit. Images should be downloaded from cameras/iPads as soon as possible and the original image deleted.
- You should not upload images or videos onto internet sites of other staff or pupils without their consent. This is applicable professionally (in school) or personally (eg staff outings).
- YouTube may be used for educational purposes. It is recommended that staff research articles and content to be used within lessons, prior to classroom use, to avoid inappropriate images being shown on school IT equipment.
- School laptops/iPads should not be used for the routine storage of personal music or photograph collections unless specific permission has been given from the Headteacher. To protect the server such files must be transferred to a portable hard drive provided by the employee as soon as possible.
- Personal use of equipment must be in the user's own time and must not impact upon work efficiency or costs
- Staff who have been given the use of a school laptop/iPad are responsible for its safekeeping both on and off site. When taken off site by car laptops/iPads should not be transported within the passenger compartment but stored securely in the boot thus reducing the risk of opportunist thefts, eg at traffic lights.
- Websites should not be created on school equipment without the written permission of the Headteacher.
- The school network must not be used for furthering outside business interests or for personal or monetary gain.
- All users have a responsibility to report any known misuse of technology including the unacceptable behaviour of others.
- Malicious Use/Vandalism – any attempt to destroy hardware, software or data will be subject to disciplinary action.
- Inappropriate media may not be used as a screensaver or background photo. Presence of pornographic materials, inappropriate language, alcohol, drug or gang related symbols or pictures will result in disciplinary actions.
- Virus outbreaks are to be reported to the ICT Technician/s-Safety Officers as soon as it is practical.
- All users have a duty to report failings of technical safeguards which may become apparent when using systems and services.
- In the event of any IT equipment provided by the school is lost, stolen or damaged the Headteacher must be notified immediately.

Use of Mobile Phones and Instant Messaging

- The use of mobile phones during lessons/after school clubs is strictly prohibited unless permission has been received from the Headteacher due to special circumstances.
- Mobile phones should not be visible in the classroom and should be placed on 'silent' mode during lessons and stored in a designated place
- Personal mobile phones should not be used to take photographs or videos unless there are exceptional circumstances and then only at the discretion of the Headteacher eg on a school visit. Images should be downloaded from the device as soon as possible and the original image deleted.
- Staff are advised not to access pupils' mobile phone numbers either to make or receive phone calls or text messages.
- Staff must not enter into instant messaging communications with pupils either by phone or social networking sites.
- Staff must not accept pupils as 'friends' on social networking sites.
- The school strongly recommends that staff should not accept parents as 'friends' on social media sites as this can lead to conflict of interest and leave staff vulnerable to inappropriate communication.

Use of iPads

Users Responsibilities

- Users must use a protective cover/case for their iPad.
- The iPad screen is made of glass and therefore is subject to cracking and breaking if misused. Never drop nor place heavy objects (books, laptops etc) on top of the iPad.
- Only a soft cloth or approved laptop screen cleaning solution is to be used to clean the iPad screen.
- Do not subject the iPad to extreme heat or cold.
- Do not store or leave unattended in vehicles.
- Users may not photograph any other person, without their consent.
- The iPad is subject to routine monitoring. Devices must be surrendered immediately upon request by a senior member of staff.
- Users in breach of this document may be subject to but not limited to disciplinary action, confiscation, removal of content or referral to external agencies in the event of illegal activity.
- Belmont School is not responsible for the financial or other loss of any personal files that may be deleted from an iPad.

Safeguarding and Maintaining as an Academic Tool

- Items deleted from the iPad cannot be recovered.
- Memory space is limited. Academic content takes precedence over personal files and apps.
- The whereabouts of the iPad should be known at all times, do not leave unattended.
- It is the user's responsibility to keep their iPad safe and secure.
- iPads belonging to other users are not to be tampered with in any manner.

Prohibited Use

- Jailbreaking – jailbreaking is the process which removes any limitations placed on the iPad by Apple. Jailbreaking results in a less secure device and is strictly prohibited

Staff should be aware that the school network and internet traffic is monitored, both at school and Lincolnshire County Council level and can be traced to an individual user. Belmont School reserves the right to confiscate and search a laptop/iPad to ensure compliance with this document. Discretion and professional conduct is essential at all times.

Appendix A

Belmont CP School
Record of Electronic Resources Used

Users must ensure electronic resources are accessed and used within applicable Copyright requirements and usage is recorded as appropriate eg music, video, online articles.

Class _____

Date	Resource used	Initial

Appendix 1

Acceptable Use of ICT – Pupils
Our Charter of Good Online Behaviour

The school has installed computers and internet access to help our learning. These rules will keep everyone safe and help us to be fair to others.

I promise:

- to only use the school ICT for educational purposes and to only access age appropriate websites
- not to look for or show other people things that may be upsetting
- to show respect for the work that other people have done

I will not:

- use other people's work or pictures without permission to do so
- damage the school's ICT equipment. If I accidentally damage something I will tell my teacher
- share my password with anybody. If I forget my password I will let my teacher know
- use other people's usernames or passwords
- share personal information online with anyone. I will not give my home address or telephone number, or arrange too meet someone, unless my parent/carer gives permission
- download anything from the internet unless my teacher has asked to me to

I will:

- let my teacher know if anybody asks me for personal information
- let my teacher know if anybody says or does anything to me that is hurtful or upsets me
- be respectful to everybody online. I will treat everybody the way that I want to be treated
- only use a memory stick in school if it has been checked by the school office for viruses
- ensure that my mobile phone is handed into the school office for safe keeping. I understand that mobile phones should not be used in school to take photographs/videos

I understand:

- that not everything on the internet is true and some people on the internet are not who they say they are, and some people can be nasty. I will tell my teacher if I am ever concerned in school, or my parents if I am at home
- if I break the rules in this charter there will be consequences in line with the Golden Rules and my parents may be informed
- that the school may check my computer files and may monitor the internet sites I visit

Pupil's Name …… Signature ……

Parent/Carer's Name …… Signature ……

Date ……

Appendix 2

Belmont Community Primary School X Accounts

This document should be read in conjunction with Belmont CP School Safeguarding Policies

Rationale

The rationale of this document is to explain acceptable use of X relating to the Belmont CP School X accounts for staff, children, parents/carers and Governors. It will therefore aim to explain the purpose of X at Belmont CP School and the benefits that will arise from its proper use, and also deal with any potential pitfalls from using social media.

Aims and Objectives

- The Belmont CP School X account will be a Public account.
- It will be used and followed principally by parent/carers, staff, Governors and other professionals in order to advertise the excellent work taking place at the school and to celebrate the success and achievements of the children.
- Individually targeted content will not be posted eg "Well done Josh a better lesson today".
- The aim of this is to run alongside more traditional methods of communication (eg letters, the school website and Parentmail), not replace them.
- Whilst using X, all staff will demonstrate safe and responsible use of social media.

X Control and Usage

The uploading of content will be controlled primarily by the Headteacher, Office Staff and e-Safety Officer. They will be responsible for password protection and uploading of content. Other members of staff may be authorised by the Headteacher. No private messages will be sent using this X account. Any contact to followers should be made using other methods.

X Followers

PUBLIC ACCOUNTS

Belmont School will:

- Monitor followers and block any who appear to not be school focused.
- Reserve the right to block accounts deemed inappropriate or offensive to ourselves and/or others.
- Delete inappropriate content that may undermine the school, its staff, parents/carers, Governors or others affiliated with the school.

Who will the Belmont CP School X Accounts follow?

The Belmont CP School X account sees itself more as a distributor of information to those who follow it and not as a receiver of information.

- In order to protect ourselves from inappropriate content being distributed into our newsfeeds, the Belmont School account will not actively seek to follow other users.
- Exceptions may be made where following a @ handle has obvious benefits to the school eg a children's author or an educationally linked account.
- The decision to follow will be dealt with on a case-by-case basis.

Inappropriate Content and Referencing

Belmont CP School welcomes any referencing, mentions, or interactions that present the school in a positive light only.

Therefore, Belmont CP School deems any of the following as inappropriate:

- Offensive language or remarks aimed at the school, its staff, parents/carers, pupils, Governors or others affiliated with the school.
- Extremist views or radical views or opinions as in line with the Prevent Duty.
- Unsuitable images or content posted into its feed.
- Unsuitable images or content finding its way from another's account into the Belmont X feeds.
- Images or text that infringe upon copyright.
- Comments that aim to undermine the school, its staff, parents/carers, Governors or others affiliated with the school.

Any inappropriate content will be deleted and its users will be removed, blocked, and, depending on the nature of the comment, reported to X. Furthermore, incidents of a more serious nature may be reported to the appropriate authority.

Tweets and Images

- The Belmont CP School X accounts will post photos of work and learning.
- It will not post photos of children's faces without the agreement of the parent/carer.
- It may share a photo of a child that features a child's hands or back of the head (for example, when creating a piece of art work).
- Pupils will not be identified by name in photos.

X's own safety rules can be read on: https://support.X.com/groups/56-policies-violations.