# CHELLINGTON CHURCH OF ENGLAND FEDERATION

**Happiness Through Wisdom**

*"Gold there is, and rubies in abundance, but lips that speak knowledge are a rare jewel."*

**Proverbs 20:15**

**St. Lawrence VA Primary School /**

**Christopher Reeves VA Primary School**

# Internet and Online Safety Policy

**March 2021**

**Review Date: March 2022**

**Statement of Intent**

ICT is an essential resource and plays an important role in the everyday lives of children, young people and adults. Consequently, the use of the Internet as a tool to develop learning and understanding has also become an integral part of school and home life.

Information and Communication Technology covers a wide range of resources including web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Apps
- E-mail, Instant Messaging and chat rooms
- Social Media, including Facebook and Twitter
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices including tablets and gaming devices
- Online Games
- Learning Platforms and Virtual Learning Environments
- Blogs and Wikis
- Podcasting
- Video sharing
- Downloading
- On demand TV and video, movies and radio / Smart TVs

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies and that some have minimum age requirements (13 years in most cases).

The Chellington Federation understand the responsibility to educate our pupils on e-Safety Issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Schools hold personal data on learners, staff and others 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 to use technology to benefit learners.

Everybody in the school community 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.

Both this policy and the Acceptable Use Agreement (for all staff, governors, regular visitors [for regulated activities] and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, mobile devices, webcams, whiteboards, digital video equipment, etc.); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones and other mobile devices).

**Incident Reporting**

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's relevant responsible individuals. Additionally, all security breaches, lost/stolen equipment or data (including remote access Secure ID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the relevant responsible individuals. The relevant responsible individuals at St Lawrence Primary School and Christopher Reeves Primary School are as follows: The Executive Headteacher, The Designated Safeguarding Lead and the Computing Subject Lead.

**Anti-virus and anti-spam system**

- The schools have an up to date anti-virus and anti-spam system provided by Partnership Education and it is monitored and updated weekly.

- If it is suspected that there may be a virus on any school ICT equipment, individuals are to stop using the equipment and contact the Computing Subject Lead immediately.

**Data Security**

The accessing and appropriate use of school data is something that the Chellington Federation takes very seriously.

**Security**

- The schools give relevant staff access to its Management Information System, with a unique username and password

- It is the responsibility of everyone to keep passwords secure

- Staff are aware of their responsibility when accessing school data

- Staff have been issued with the relevant guidance documents and the Policy for ICT Acceptable Use

- Staff keep all school related data secure. This includes all personal, sensitive, confidential or classified data

- Staff should avoid leaving any portable or mobile ICT equipment or removable storage media in unattended vehicles.

- It is the responsibility of individual staff to ensure the security of any personal, sensitive, confidential and classified information contained in documents faxed, copied, scanned or printed. This is particularly important when shared copiers (multi-function print, fax, scan and copiers) are used

**Managing e-mail**

- The Chellington Federation gives all staff & governors their own e-mail account to use for all school business as a work based tool. This is to protect staff, minimise the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal profile information being revealed

- Staff & governors should use their federation email for all professional communication.

- It is the responsibility of each account holder to keep the password secure. For the

safety and security of users and recipients, all mail is filtered and logged; if necessary e-mail histories can be traced. The school email account should be the account that is used for all school business

- Under no circumstances should staff contact pupils, parents or conduct any school business using personal e-mail addresses

- Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes

- Staff must inform the Computing Subject Lead or their line manager if they receive an offensive e-mail

- Pupils are introduced to e-mail as part of the Computing Programme of Study and monitored accordingly.

**Online-Safety in the Curriculum**

ICT and online resources are increasingly used across the curriculum. We believe it is essential for Online-Safety guidance to be given to the pupils on a regular and meaningful basis. Online-Safety is embedded within our curriculum and we continually look for new opportunities to promote Online-Safety.

- Both schools have a framework for teaching internet skills in Computing lessons

- The school provides opportunities within a range of curriculum areas to teach about Online-Safety

- Educating pupils about the online risks that they may encounter outside school is done informally, when opportunities arise and as part of the Online-Safety curriculum

- Pupils are taught about copyright, respecting other people's information, safe use of images and other important areas through discussion, modeling and appropriate activities

- Pupils are made aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. Pupils are also made aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Cyber Mentors, ChildLine or CEOPS report abuse button

**Online-Safety Skills Development for Staff**

- Our staff receive information and training on Online-Safety and how they can promote the 'Stay Safe' online messages

- New staff receive information on the school's acceptable use policy as part of their induction

- All staff have been made aware of their individual responsibilities relating to the safeguarding of children within the context of Online-Safety and know what to do in the event of misuse of technology by any member of the school community

- All staff are expected to incorporate Online-Safety activities and awareness within their curriculum areas and ensure they are adequately informed with up-to-date areas of concern.

**Managing the School Online-Safety Messages**

- We endeavour to embed Online-Safety messages across the curriculum whenever the internet and/or related technologies are used
- The Online-Safety policy will be introduced to the pupils at the start of each school year
- The key Online-Safety advice will be promoted widely through school displays, newsletters, class activities and so on
- We will participate in Safer Internet Day each year

**Internet Use**

The internet is an open worldwide communication medium, available to everyone, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people.

Managing the Internet

- The school provides pupils with supervised access to Internet resources through the school's internet connectivity
- Staff will preview any recommended sites, online services, software and apps before use
- Searching for images through open search engines is discouraged when working with pupils
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents re-check these sites and supervise this work. Parents will be advised to supervise any further research
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources
- All users must observe copyright of materials from electronic resources
- The federation utilises a content filter to ensure that all web-based content is suitable for the age range of the children at the school. In addition to this, the Hector the Dolphin safety button is installed on all school devices to ensure that if any content does upset or distress a child they are able to deactivate this content immediately and report it. All children at the school are made familiar with this use of this tool

**Parental Involvement**

We believe that it is essential for parents/carers to be fully involved with promoting Online-Safety both in and outside of school and to be aware of their responsibilities. We consult and discuss Online-Safety with parents/ carers and seek to promote a wide understanding of the benefits of new technologies, together with the associated risks.

- Parents/carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to the schools

- Parents/carers are required to make a decision as to whether they consent to images of their child being taken and used in the public domain (e.g., on school website or Facebook page.)

- Parents/carers are expected to sign a Home-School agreement

- The school disseminates information to parents relating to Online-Safety where appropriate in the form of;

    - Information evenings
    - Practical training sessions e.g. current Online-Safety issues
    - Posters
    - School website information
    - Newsletter items
    - Information home by email

**Protecting Personal, Sensitive, Confidential and Classified Information**

- Ensure that any school information accessed from your own PC or removable media equipment is kept secure, and remove any portable media from computers when not attended.
- Ensure you lock your screen before moving away from your computer during your normal working day to prevent unauthorised access
- Ensure the accuracy of any personal, sensitive, confidential and classified information you disclose or share with others
- Ensure that personal, sensitive, confidential or classified information is not disclosed to any unauthorised person
- Ensure the security of any personal, sensitive, confidential and classified information contained in documents you fax, copy, scan or print. This is particularly important when shared copiers (multi-function print, fax, scan and copiers) are used and when access is from a non-school environment
- You must not post on the internet any personal, sensitive, confidential, or classified information, or disseminate such information in any way that may compromise its intended restricted audience

**Preventing radicalization**

The government statutory guidance makes clear the need for schools to ensure that children are safe from terrorist and extremist material when accessing the internet in schools. The school ensures that suitable filtering is in place and more generally, all staff work to equip children and young people with the knowledge to stay safe online, both in school and outside. Internet safety is integral to our ICT curriculum as well as other parts of the curriculum such as PSHE and British Values. As with other online risks of harm, every staff member, governor or other adult associated with the school, is made aware of the risks posed by the online activity of extremist and terrorist groups. This is carried out with regular PREVENT training facilitated by Bedford Borough Council.

**Safe Use of Images**

**Taking of Images and Film**

Digital images are easy to capture, reproduce and publish and, therefore, misuse. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.

- With the written consent of parents (on behalf of pupils) and staff, the schools permit the appropriate taking of images by staff and pupils with school equipment
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on field trips and, as per the Safeguarding Policy and Mobile Phone Policy, personal mobile phones are not permitted in the classrooms whilst pupil are present.
- Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of pupils, staff and other with advance permission from the Executive Headteacher.
- Pupils and staff must have permission from the Executive Headteacher before any image can be uploaded for publication.

**Publishing Pupil's Images and Work**

On a child's entry to the schools all parents/carers will be asked to give permission to use their child's work/photos in the following ways:

- On the school website
- in the school prospectus and other printed publications that the school may produce for promotional purposes
- recorded/ transmitted on a video or webcam

  in display material that may be used in the school's communal areas
- in display material that may be used in external areas, i.e. exhibition promoting the school
- general media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)
- in publicity for or resulting from inter-school activities held either on site or at another venue

This consent form is considered valid for the entire academic year unless there is a change in the child's circumstances where consent could be an issue.

Parents or carers may withdraw permission, in writing, at any time. Consent must also be given in writing and will be kept on record by the school.

Pupils' names will not be published alongside their image and vice versa. E-mail and postal addresses of pupils will not be published. Pupils' full names will not be published.

Before posting identifiable student work on the Internet, a check needs to be made to ensure that permission from the parent/carer has been given for work to be displayed.

**Storage of Images**

- Images/ films of children are stored on the school's secure server
- Images/films of children are to be removed at the end of the academic year in which that child leaves the school, unless such images/ films are or have been used for the purposes of promoting the school.

**Confirmation**

This policy was reviewed and agreed in full by the Governing Body:

Signed: ……..
Chair of Governors

Date: …….
Date of next review: March 2022