Burton Agnes C of E Primary School

E safety Policy

September 2025

Burton Agnes C of E School E Safety Policy

Rationale

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

At Burton Agnes School, we understand that we have a responsibility to educate our pupils on e-safety issues; teaching them the appropriate behaviours and 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.

Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognize 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
- Learning Platforms and Virtual Learning Environments
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality

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.

Aims

- To provides opportunities within a range of curriculum areas to teach about e-safety.
- To educate pupils on the dangers of technologies that they may encounter outside of school. This will be done both informally when opportunities arise and as part of the e-safety curriculum.
- To make pupils aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them.

- To teach pupils about respecting other people's information, images, etc through discussion, modeling and activities.
- To make pupils aware of online bullying and know how to seek help if they are affected by these issues. Pupils will also be made aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. class teacher /e-safety coordinator/head-teacher.
- To critically evaluate the materials they find and learn good searching skills through the ICT curriculum.

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

Roles and Responsibilities

As e-safety is an important aspect of strategic leadership within the school, the Head and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named e-safety co-ordinator in our school is Mrs Jameson. It is the role of the e-safety co-ordinator to keep abreast of current issues and guidance through organisations such as East Riding Safeguarding of Children Board, Becta, CEOP (Child Exploitation and Online Protection) and Childnet. This policy, supported by the school's acceptable use agreements for staff, governors, visitors and pupils (appendices), is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, health and safety, home–school agreements, and behaviour (including the anti-bullying) policy.

Role of the E-safety Co-ordinator

1) To provide leadership, expertise, advice and assistance for members of staff.
2) To develop and implement appropriate record keeping on any e-safety issues
3) To ensure that the policy for e-safety is regularly evaluated and up dated, is known and understood by staff and provides continuity and development throughout the school.
4) To liaise with governors as appropriate in particular the governor for e-safety.
5) To monitor and assess standards and quality of teaching and learning using observations, standardized data, monitoring of work and lessons. From this to know strengths and weaknesses of implementation of e-safety throughout the school.
6) To be aware of, and identify, INSET needs - making use of expertise available inside the school, liaise with the LEA e-safety Officer and through organizations such as The Child Exploitation and Online Protection (CEOP).
7) To be conversant with current thinking and developments in understanding and delivering e-safety messages. The school's e-Safety coordinator ensures the Governors are updated as necessary.

E-safety skills development for staff

- Our staff receive regular information and training on e-safety issues.
- New staff receive information on the school's acceptable use and e-safety policies as part of their induction.
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of e-safety and know what to do in the event of misuse of technology by any member of the school community.
- All staff are encouraged to incorporate e-safety activities and awareness within their curriculum areas.

Managing the school E-Safety messages

- We endeavour to embed e-safety messages across the curriculum whenever the internet and/or related technologies are used.
- The e-safety policy will be introduced to the pupils at the start of each school year.
- E-safety information will be available via the school website

Password Security

Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords which are not shared with anyone. The pupils are educated about choosing suitable passwords although their files in school are just stored under class log ins. Staff and pupils are regularly reminded of the need for password security.

- All users read and agree to abiding by an Acceptable Use Agreement to demonstrate that they have understood the school's e-safety policy. .
- Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks, including ensuring that passwords are not shared and are changed periodically.

Individual staff users must also make sure that workstations are not left unattended, or are locked. The internet is an open communication medium, available to all, 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.

How will information systems security be maintained?

Data security is very important and the the Headteacher is the person in charge of data security/GDPR and is known within the school. The role is distinct and separate from the 'Esafety co-ordinator. All staff with access to personal data are liable in law to protect that data. Should data be lost from an unencrypted USB drive or seen on a laptop used by other people, the consequences could be serious for the member of staff, for the school or organisation.

Local Area Network (LAN) security issues include:

• Access to all ICT systems shall be via unique login and password. Any exceptions shall be recorded in the risk assessment and approved by the person in charge of data security.
• Where possible, all information storage shall be restricted to only necessary users. Access granted to new groups of users (for example, an external group attending a school-based event) shall be approved by the person in charge of data security.
• All requests for access beyond that normally shall be authorised by the person in charge of data security. This shall include the authorisation of access required by the ICT Support Team during investigations.
• Where 'restricted' information is stored, access shall only be granted to individuals approved by the person in charge of data security. A record shall be kept of these approvals.
• All access controls should be reviewed each term, to ensure that any users that leave have their access removed.
• Users will act reasonably — e.g. the downloading of large files during the working day will affect the service that others receive.
• Users will take responsibility for their network use.
• The server operating system will be secured and kept up to date.
• Virus protection for the whole network will be installed and current.
• Access by wireless devices will be pro-actively managed and will be password protected.
• Portable media may not be used without specific permission followed by a virus check.
• Unapproved software will not be allowed in pupils'/staff work areas or attached to email.
• Files held on the organisation's network will be regularly checked.
• The person in charge of network management will review system capacity regularly.
• All staff laptops are bit locked Infrastucture • School internet access is controlled through the East Riding's web filtering service.
• Burton Agnes School is aware of its responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 1998, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998.
• Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required.
• If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported via the 'Internet log' found in the school office. The sheet is then handed immediately to the e-safety co-ordinator..
• It is the responsibility of the school to ensure that anti-virus protection is installed and kept up-to-date on all school machines. If there are any issues related to viruses or anti-virus software, the Head Teacher should be informed immediately.
• Pupils and Staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-

to-date virus protection software. It is not the school's responsibility or the resource technician to install or maintain virus protection on personal systems.

- Pupils and staff are not permitted to download programs or files on school based technologies without seeking prior permission of the head teacher. Special Educational Needs, Inclusion and Equal Opportunities
- The school endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the schools' esafety rules. However, staff are aware that some pupils may require additional teaching including (visual) reminders, prompts and further explanation to reinforce their existing knowledge and understanding of e-safety issues.
- Where a pupil has poor social understanding or Special Educational Needs careful consideration is given to group interactions when raising awareness of e-safety. Internet activities are planned and well managed for these children and young people. Managing Web 2.0 Technologies Pupils
- At present, Burton Agnes endeavours to deny access to social networking sites to pupils within school and to deter them from accessing adult social networking sites out of school.
- All pupils are advised to be cautious about the information given by others on sites, for example users not being who they say they are.
- Pupils are taught to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.
- Pupils are always reminded to avoid giving out personal details on such sites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/ email address, specific hobbies/ interests).
- Pupils are encouraged to be wary about publishing specific and detailed private thoughts online.
- Pupils are reminded that posting material which may be construed as offensive relating to the school, pupils or staff, on any internet site is considered by the school as cyberbullying and appropriate action will be taken.
- Any video/images taken that show the school site and/or students in school uniform are considered to be inappropriate for uploading to the internet unless the permission of the Head Teacher has first been given.
- Our pupils are asked to report any incidents of bullying to the school via their class teacher.

Staff

- Staff are advised to employ caution when posting any material on the internet relating to themselves and their activities. The golden rule is to ensure that there would be no embarrassment or other consequences if something posted were read by the Head Teacher or pupils of the school.
- Staff are advised that, once posted on the internet, personal material may be publicly available for many years. All staff, and especially new staff, are therefore advised to

check that no material about themselves can be found on the internet that would not meet the golden rule.

- (Remember that sometimes your image may be 'tagged' by other friends and acquaintances).
- Staff are advised to use social networking and other similar sites (eg YouTube/Face book etc) only with caution and to use the security features to ensure maximum privacy settings. Under no circumstances are staff allowed to accept a student as a 'friend' on any personal social networking site unless that student is a close relative (ie son/daughter/brother/sister etc). When posting, even with maximum privacy settings, staff are advised to remember the golden rule.
- Staff are advised only to create blogs, wikis or other web 2.0 spaces for educational purposes using the School Learning Platform where appropriate.
- Any video/images taken that show the school site and/or students in school uniform are considered to be inappropriate for uploading to the internet (whether for educational purposes or not) unless the permission of the Head Teacher has first been given.

Mobile technologies Personal Mobile devices (including phones)

- The school allows staff to bring in personal mobile phones and devices for their own use.
- Pupils are not allowed to bring personal mobile devices/phones to school but in circumstances where this is unavoidable the mobile device will be stored in the school office and collected at the end of the school day.
- This technology may be used, on occasion for educational purposes. The device user, in this instance, must always ask the prior permission of the bill payer.
- The school is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate text messages between any member of the school community is not allowed.
- Permission of the subject(s) must be sought before any image or sound recordings are made on these devices of any member of the school community.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.
- Staff must not take photos of pupils on their mobile phones. School provided Mobile devices (cameras and digital video cameras) The sending of inappropriate text messages between any member of the school community is not allowed.
- Permission of the subject(s) must be sought before any image or sound recordings are made on the devices of any member of the school community.
- Where the school provides mobile technologies such as laptops and video cameras for offsite visits and trips, only these devices should be used.

Managing Email

The use of email within most schools is an essential means of communication for both staff and pupils. In the context of school, email should not be considered private.

Educationally, email can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or international. We recognise that pupils need to understand how to style an email in relation to their age and good 'netiquette'.

- It is the responsibility of each account holder to keep their password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary email histories can be traced. This should be the account that is used for all school business.
- Under no circumstances should staff contact pupils or parents using personal email addresses.
- E-mail sent to an external organisation should be written carefully before sending, in the same way as a letter written on school headed paper.
- All e-mail users are expected to adhere to the generally accepted rules of network etiquette ('netiquette'). This is particularly in relation to the use of appropriate language, not revealing any personal details about themselves or others in e-mail communication, never arranging to meet anyone without specific permission and virus checking attachments.
- Pupils must immediately tell a teacher/ trusted adult if they receive an offensive email (do not delete the email as it will be needed as evidence). This should be reported to the class teacher who may decide to forward this for action to the headteacher.
- Staff must inform the head teacher if they receive an offensive e-mail.
- Pupils are introduced to email as part of the ICT Scheme of Work. 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 school permits 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.
- Where possible general shots of classroom or group activities should be taken rather than close-up shots of individual pupils. Care should be taken to ensure that students are in suitable dress (particularly relevant for PE activities). Staff should also be mindful of including images of children from different ethnic backgrounds and with disabilities to promote the school as an inclusive community and to comply with the Disability Discrimination Act.
- The Foundation staff will of course have to take individual photographs as evidence for the children's profiles. Publishing pupil's images and work On a child's entry to the school, and on an annual basis after that date, all parents/carers will be asked to give permission to take photos for work in school and on the internet. Parents/ carers may withdraw permission, in writing, at any time. Pupils' full names will not be published on the school website.

Online Safety and Filtering and Monitoring

The importance of safeguarding children from potentially harmful and inappropriate online material is recognised and understood, along with the fact that technology is a significant component in many safeguarding and wellbeing issues.

To address this and in light of the 4 categories of risk outlined below, we will adopt a whole school approach involving a number of measures and approaches with the aim of:

- Having robust processes (including filtering and monitoring systems) in place to ensure the online safety of pupils, staff, volunteers and governors
- Protecting and educating the whole school community in safe and responsible use of technology, including mobile and smart technology
- Setting clear guidelines for the use of mobile phones for the whole school community
- Establishing clear mechanisms to identify, intervene in and escalate any incidents or concerns, where appropriate

The approach to online safety is based on addressing the following 4 categories of Risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

KCSiE 2023, outlines the need for staff and Governors to receive training covering online safety (including Filtering and Monitoring) and that it is essential that there is a whole school approach towards online safety, spanning training, curriculum content and teaching, communication with parents/carers and school IT resources / devices / network (appropriate filtering and monitoring etc). The Governing Body will retain strategic oversight of this and ensure that appropriate processes and procedures are established and maintained.

The Governing Body will

- Make sure that the school has appropriate filtering and monitoring systems in place and review their effectiveness
- Review the DfE's filtering and monitoring standards, and discuss with IT staff and service providers about what needs to be done to support the school to meet these standards
- Make sure the DSL takes lead responsibility for understanding the filtering and monitoring systems in place as part of their role
- Make sure that all staff undergo safeguarding and child protection training, including online safety and that such training is regularly updated and is in line with advice from the safeguarding partners
- Make sure staff understand their expectations, roles and responsibilities around filtering and monitoring as part of safeguarding training

In relation to filtering and monitoring, we will adhere to DfE filtering and monitoring standards on school devices and school networks, and in so doing will:

• identify and assign roles and responsibilities to manage filtering and monitoring systems.

• review filtering and monitoring provision at least annually.

• block harmful and inappropriate content without unreasonably impacting teaching and learning.

• have effective monitoring strategies in place that meet their safeguarding needs

have established mechanisms to identify, intervene in, and escalate any concerns where appropriate.

Burton Agnes work closely with East riding Schools ICT who regularly check and monitor smoothwall sysyems.

Adherence to the standards will be regularly reviewed (at least annually) and involve discussion with IT staff and service providers and the nominated Governor and SLT member for this area of safeguarding as well as the DSL (who will lead and retain responsibility for this). This will be supported by an annual risk assessment that considers and reflects the risks faced by our school community.

As part of their oversight role, our Governing body will ensure staff safeguarding and child protection training includes online safety which, amongst other things, includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring.

Filtering breaches or concerns identified through internal monitoring will be recorded and reported to the DSL, who will review and respond as appropriate. The DSL will respond to online safety concerns in line with Safeguarding / Child Protection and any other associated policies, including our Anti-bullying policy and Behaviour Policy:

- Internal sanctions and/or support will be implemented as appropriate.

- Where necessary, concerns will be escalated and reported to relevant partner agencies in line with local policies and procedures.

Burton Agnes CE Primary School uses a wide range of devices and technology systems to facilitate internal and external communication, teaching and information storage. The school Acceptable User Policy underpins the operation of all school owned devices and systems along with safety and security measures in place.

All communication with pupils/students and parents/carers will take place using School/College provided or approved communication channels; for example, School/College provided email accounts and phone numbers and/or agreed systems: Google Classroom, Microsoft 365 or equivalent etc. Any pre-existing relationships or situations which mean this cannot be complied with will be discussed with the DSL.

Any access to materials believed to be illegal, will be considered as a safeguarding issue and appropriate action taken to address concerns

EYFS staff will use learning book as a method of recording progress. Parents have signed an agreement to use this.

Video Conferencing • Permission is sought from parents and carers if their children are involved in video conferences with people from outside the school setting.

- All pupils are supervised by a member of staff when video conferencing
- The school keeps a record of video conferences, including date, time and participants.

Parental right to take photographs and videos

Parents are permitted to take photographs and videos at school events for their own personal use only (unless this is expressly prohibited – for example at school plays where there are third party copyright regulations which prohibit recordings). Recording and/or photographing other than for private use would require the consent of other parents whose children may be captured on film. Without this consent, the Data Protection Act 1988 would be breached.

Official School Photographs

From time to time the school will invite an official photographer into school to take photographs of individual children and class groups. The school will ensure that appropriate CRB checks have been made with the company concerned. Misuse and Infringements Complaints and Reports Complaints and reports relating to e-safety should be made to the Head Teacher who will then liaise with other members of staff/students/parents as appropriate. All incidents will be logged and appropriate action taken and recorded.

Sanctions

A variety of sanctions may be used according to the type and seriousness of the incident. These may include, but are not limited to:

- An internet ban for a fixed period

- A ban from the school network for a fixed period
- Parents
- A verbal/written warning
- Exclusion for a fixed period
- Permanent exclusion
- Any sanction needs to be mindful of our Christian nature, the need to learn from mistakes and move on. Inappropriate material
- All users are made aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the Head Teacher.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the Head Teacher, depending on the seriousness of the offence; investigation by the Headteacher/ LA, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences.
- Users are made aware of sanctions relating to the misuse or misconduct of the school computer network as part of the acceptable use policy. Parental Involvement We believe that it is essential for parents/ carers to be fully involved with promoting esafety both in and outside of school. We regularly consult and discuss e-safety with parents/ carers and seek to promote a wide understanding of the benefits related to ICT and associated risks.
- Parents/ carers and pupils are actively encouraged to contribute to adjustments or reviews of the school e-safety policy by contacting the Head Teacher to discuss esafety issues.
- Parents/ carers are required to make a decision as to whether they consent to images of their child being taken/ used in the public domain (e.g., on school website)
- The school disseminates information to parents relating to e-safety where appropriate in the form of;
  - o Displays and posters
  - o Website/ Learning Platform postings
  - o Newsletter items

- There will be an on-going opportunity for staff to discuss with the Head Teacher any issue of e-safety that concerns them.
- This policy will be reviewed every 12 months and consideration given to the implications for future whole school development planning.

This policy will be reviewed in September 2026