Bassingbourn Community Primary School
E safety Policy

This policy was ratified on: 17th July 2025

Implemented on: 17th July 2025

Review date: July 2026

1. Introduction and Overview

Rationale

The purpose of this policy is to:

- set out the key principles expected of all members of the school community at Bassingbourn Community Primary School with respect to the use of ICT-based technologies (including data protection and the management of information).
- safeguard and protect the children and staff of Bassingbourn Community Primary School.
- assist school staff working with children to work safely and responsibly with the Internet and other communication technologies and to monitor their own standards and practice.
- set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use.
- have clear structures to deal with online abuse such as cyberbullying which are cross referenced with other school policies.
- ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- minimise the risk of misplaced or malicious allegations made against adults who work with students.

The main areas of risk for our school community can be summarised as follows.

Content

- exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse
- lifestyle websites, for example pro-anorexia/self-harm/suicide sites
- hate sites
- content validation: how to check authenticity and accuracy of online content

Contact

- grooming
- cyber-bullying in all forms
- identity theft (including 'frape' (hacking Facebook profiles)) and sharing passwords. Impersonation.

Conduct

- privacy issues, including disclosure of personal information
- digital footprint and online reputation
- health and well-being (amount of time spent online (Internet or gaming))
- sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images)
- copyright (little care or consideration for intellectual property and ownership – such as music and film)
- Aggressive behaviours (bullying, Cyberbullying and Self-bullying)

Scope

This policy applies to all members of the Bassingbourn Primary community (including staff/governors, students/pupils, volunteers, parents/carers, visitors,

community users) who have access to and are users of the school's IT systems, both in and out of Bassingbourn Primary School.

Roles and responsibilities

Role	Key Responsibilities
Headteacher	• To take overall responsibility for e-safety provision • To take overall responsibility for data and data security (SIRO – Senior Information Risk Officer) • To ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements • To be responsible for ensuring that staff receive suitable training to carry out their e-safety roles and to train other colleagues, as relevant • To be aware of procedures to be followed in the event of a serious e-safety incident. • To ensure that there is a system in place to monitor and support staff who carry out internal e-safety procedures • To receive regular monitoring reports from the E-Safety Co-ordinator / Officer

E-Safety Co-ordinator (Matthew Bryant)
 	
Designated Safeguarding Lead (Amy Luu)
	• Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
	• Promotes an awareness and commitment to e-safeguarding throughout the school community
	• Ensures that e-safety education is embedded across the curriculum
	• Liaises with school ICT technical staff
	• Communicates regularly with SLT and the designated Safeguarding Governor / committee to discuss current issues, review incident logs and filtering / change control logs
	• Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident
	• Ensures that an e-safety incident log is kept up to date – forms available in staff room. To be returned to e-safety co-ordinator.
	• Facilitates training and advice for all staff
	• Liaises with the Local Authority and relevant agencies
	• Conduct any pupil surveys / pupil feedback on online safety issues
	• Is regularly updated in e-safety issues and legislation, 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 and use of social media

Governors	• Ensures that the school follows all current e-safety advice to keep the children and staff safe • Supports the school in encouraging parents and the wider community to become engaged in e-safety activities

Role	Key Responsibilities
	• Approves the E-Safety Policy and review the effectiveness of the policy. This will be carried out by the Governors receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of E-Safety/Safeguarding Governor The role of the E-Safety Governor will include: • regular review with the E-Safety Co-ordinator / Officer (including e-safety incident logs, filtering / change control logs)
Computing Curriculum Leader	• Oversees the delivery of the e-safety element of the Computing curriculum (also in relation to PSHE modules) • Liaises with the e-safety coordinator regularly
Operations Manager	• Reports any e-safety related issues that arises, to the e-safety coordinator. • Ensures that users may only access the school's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed • Ensures that provision exists for misuse detection and malicious attack e.g. keeping virus protection up to date) • Ensures the security of the school ICT system • Ensures that access controls / encryption exist to protect personal and sensitive information held on school-owned devices • Ensures the school's policy on web filtering is applied and updated on a regular basis • Ensures the appropriate body is informed of issues relating to the filtering • Keeps up to date with the school's e-safety policy and technical information to effectively carry out their e-safety role and to inform and update others as relevant • Ensures appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster • Keeps up-to-date documentation on the school's e-security and technical procedures • To ensure that all data held on pupils on the school office machines have appropriate access controls in place • To ensure that the data they manage is accurate and up to date • Ensure best practice in information management. i.e. have appropriate access controls in place, that data is used, transferred and deleted in-line with data protection requirements.
Teachers	• To embed e-safety issues in all aspects of the curriculum and other school activities • To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant) • To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws • Ensures that the use of any learning platform is regularly monitored in order that any misuse / attempted misuse can be reported to Computing Coordinator and E-Safety Co-ordinator

Role	Key Responsibilities
All staff (this section also applies to Governors)	• To read, understand and help promote the school's e-safety policies and guidance • To read, understand, sign and adhere to the school staff Acceptable Use Agreement / Policy • To be aware of e-safety issues related to the use of mobile phones, cameras and handheld devices and that they monitor their use and implement current school policies regarding these devices • To report any suspected misuse or problem to the e-safety coordinator • To maintain an awareness of current e-safety issues and guidance e.g. through CPD • To model safe, responsible and professional behaviours in their own use of technology • To ensure that any digital communications with pupils should be on a professional level and only through school-based systems, never through personal mechanisms, e.g. email, text, mobile phones etc.
Pupils	• Read, understand, sign and adhere to the Pupil Acceptable Use Policy (at KS1 it would be expected that parents / carers would sign on behalf of the pupils) • Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations • Understand the importance of reporting abuse, misuse or access to inappropriate materials • Know what action to take if they or someone they know feels worried or vulnerable when using online technology. • Know and understand school policy on the use of mobile phones, digital cameras and handheld devices. • Know and understand school policy on the taking / use of images and on cyber-bullying. • 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 • Take responsibility for learning about the benefits and risks of using the Internet and other technologies safely both in school and at home • Help the school in the creation/ review of e-safety policies
Parents/carers	• Support the school in promoting e-safety and endorse the Acceptable Use Agreement which includes the pupils' use of the Internet and the school's use of photographic and video images • Read, understand and promote the school Pupil Acceptable Use Agreement with their children • Access the school website / on-line student / pupil records in accordance with the relevant school Acceptable Use Agreement. • To consult with the school if they have any concerns about their children's use of technology
External groups	• Any external individual / organisation will sign an Acceptable Use Policy prior to using any equipment or the Internet within school • To support the school in promoting online safety

Role	Key Responsibilities
	• To model safe, responsible and positive behaviours in their own use of technology.

Communication:
The policy will be communicated to staff/pupils/community in the following ways:

- Policy to be posted on the school website and copies to be kept in the policy file found in Headteachers' office. Policy to be uploaded to the staff share area policy file.
- Policy to be part of school induction pack for new staff
- Acceptable use agreements discussed with pupils at the start of each year
- Acceptable use agreements to be issued to whole school community, usually on entry to the school
- Acceptable use agreements to be held in pupil and personnel files
- Acceptable use agreements to be displayed in each classroom and on laptop/ipad trolleys.

Handling complaints:
- The school will take all reasonable precautions to ensure e-safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.
- Staff and pupils are given information about infringements in use and possible sanctions.

  <u>Sanctions available include:</u>
- Interview/counselling by class teacher/ E-Safety Coordinator / Headteacher;
- Informing parents or carers;
- Removal of Internet or computer access for a period, [which could ultimately prevent access to files held on the system, including examination coursework];
- Referral to LA / Police.
- Our E-Safety Coordinator acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher.
- Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school / LA child protection procedures.

Review and Monitoring
The e-safety policy is referenced from within other school policies: Computing policy, Child Protection policy, Anti-Bullying policy and in the School Development Plan, Behaviour policy, Personal, Social and Health Education policies.
- The school has an e-safety coordinator who will be responsible for document ownership, review and updates.
- The e-safety policy will be reviewed annually or when any significant changes occur regarding the technologies in use within the school
- The e-safety policy has been written by the school e-safety Leader and is current and appropriate for its intended audience and purpose.

- The policy has been approved by Governors. All amendments to the school e-safeguarding policy will be shared with all staff.

2. Education and Curriculum

Pupil e-safety curriculum

This school

- Has a clear, progressive e-safety education programme as part of the Computing curriculum / PSHE curriculum. This covers a range of skills and behaviours appropriate to their age and experience, including:
    - To STOP and THINK before they CLICK
    - To develop a range of strategies to evaluate and verify information before accepting its accuracy;
    - To be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be;
    - To know how to narrow down or refine a search;
    - [For older pupils] to understand how search engines work and to understand that this affects the results they see at the top of the listings;
    - To understand acceptable behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private;
    - To understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
    - To understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments;
    - To understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings;
    - To understand why they must not post pictures or videos of others without their permission;
    - To know not to download any files – such as music files - without permission;
    - To have strategies for dealing with receipt of inappropriate materials;
    - [For older pupils] to understand why and how some people will 'groom' young people for sexual reasons;
    - To understand the impact of cyberbullying, sexting and trolling and know how to seek help if they are affected by any form of online bullying.
    - To know how to report any abuse including cyberbullying; and how to seek help if they experience problems when using the Internet and related technologies, i.e. parent or carer, teacher or trusted staff member, or an organisation such as ChildLine or the CLICK CEOP button.

- Plans internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- Will remind students about their responsibilities through an end-user Acceptable Use Policy which every student will receive and will be displayed throughout the school.
- Ensures staff will model safe and responsible behaviour in their own use of technology during lessons.

- Ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and know that they must respect and acknowledge copyright / intellectual property rights.
- The e-safety curriculum will be delivered through half termly e-safety lessons, e-safety day and through esafety assemblies (both whole school and key stage assemblies).
- Ensures that staff and pupils understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include risks in pop-ups; buying on-line; on-line gaming / gambling.

Staff and governor training

This school

- Ensures staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection;
- Makes regular training available to staff on e-safety issues and the school's e-safety education program; annual updates/ regular staff meetings etc.
- Provides, as part of the induction process, all new staff [including those on university/college placement and work experience] with information and guidance on the e-safeguarding policy and the school's Acceptable Use Policies.

Parent awareness and training

This school

- Runs a rolling programme of advice, guidance and training for parents, including:
    - Introduction of the Acceptable Use Agreements to new parents, to ensure that principles of e-safe behaviour are made clear
    - suggestions for safe Internet use at home through half-termly e-safety newsletters;
    - provision of information about national support sites for parents.

3. Expected Conduct and Incident management

Expected conduct

In this school, all users:

- Are responsible for using the school ICT systems in accordance with the relevant Acceptable Use Policy which they will be expected to sign before being given access to school systems. (at Early Years and KS1 it would be expected that parents/carers would sign on behalf of the pupils.)
- Need to understand the importance of misuse or access to inappropriate materials and are aware of the consequences
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- 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
- Will be expected to know and understand school policies on the use of mobile phones, digital cameras, hand held and other electronic devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying

Staff (including governors)

- Are responsible for reading the school's policies and using the school ICT systems accordingly, including the use of mobile phones, and hand held devices.

Students/Pupils

- Should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

Parents/Carers

- Should provide consent for pupils to use the Internet, as well as other technologies, as part of the e-safety acceptable use agreement form at time of their child's entry to the school
- Should know and understand what the 'rules of appropriate use' are and what sanctions result from misuse

Governors

- Monitor the occurrence of poor e-safety behaviour via Health and Safety Governors committee reports.
- Ensure action by the school to tackle any occurrences of poor e-safety behaviour.

Incident Management

In this school:

- There is strict monitoring and application of the e-safety policy and a differentiated and appropriate range of sanctions, though the attitudes and behaviour of users are generally positive and there is rarely needed to apply sanctions
- All members and its wider community are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes / critical incident policy.
- Support is actively sought from other agencies as needed (e.g. the local authority and regional broadband grid, UK Safer Internet Centre helpline) in dealing with e-safety issues CEOP, Prevent Officer, Police, Internet Watch Foundation) in dealing with online safety issues
- Monitoring and reporting of e safety incidents takes place and contribute to developments in policy and practice in e-safety within the school
- Parents / carers are specifically informed of e-safety incidents involving young people for whom they are responsible
- We will contact the Police if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law
- We will immediately refer any suspected illegal material to the appropriate authorities – Police, Internet Watch Foundation and inform the LA.

4. Managing the ICT infrastructure

- **Internet access, security (virus protection) and filtering**

This school:

- Has the educational filtered secure broadband connectivity through the LGfL and so connects to the 'private' National Education Network;
- Uses the Cambridgeshire ICT services filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc. All changes to the filtering policy are logged and only available to staff with the approved 'web filtering management' status;
- Ensures network healthy through use of anti-virus software etc. and network set-up so staff and pupils cannot download executable files;
- Uses DfE, LA approved systems, secured email to send personal data over the Internet and uses encrypted devices or secure remote access where staff need to access personal level data off-site;
- Has blocked pupil access, on iPads, to music download or shopping sites – except those approved for educational purposes at a regional or national level.
- Works in partnership with Cambridgeshire ICT services to ensure any concerns about the system are communicated so that systems remain robust and protect students;
- Is vigilant in its supervision of pupils' use at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access;
- Ensures all staff and students have signed an acceptable use agreement form and understands that they must report any concerns;
- Ensures pupils only publish within an appropriately secure environment.
- Requires staff to preview websites before use [where not previously viewed or cached] and encourages use of the school's Learning Platform as a key way to direct students to age / subject appropriate web sites; Plans the curriculum context for Internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required; e.g. yahoo for kids or ask for kids , Google Safe Search etc. Kids-search
- Is vigilant when conducting 'raw' image search with pupils e.g. Google image search;
- Informs all users that Internet use is monitored;
- Informs staff and students that that they must report any failure of the filtering systems directly to the class teacher who would escalate concerns to E-safety co-ordinator. Our system administrator(s) logs or escalates as appropriate to the Technical service provider or Cambridgeshire ICT Helpdesk as necessary;
- Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through staff meetings and teaching programme;
- Provides advice and information on reporting offensive materials, abuse/ bullying etc. available for pupils, staff and parents
- Immediately refers any material we suspect is illegal to the appropriate authorities – Police – and the LA.

- **Network management (user access, backup)**
  This school
  - Uses individual, audited log-ins for all users .
  - Uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services.
  - Ensures the Systems Administrator is up-to-date with relevant Cambridgeshire LA services and policies;

- Storage of all data within the school will conform to the UK data protection requirements
- Pupils and Staff using mobile technology, where storage of data is online, will conform to the EU data protection directive where storage is hosted within the EU.

To ensure the network is used safely, this school:

- Ensures staff read and sign that they have understood the school's e-safety Policy. Following this, they are set-up with Internet, email access and network access. Online access to service is through a unique, audited username and password. We also *provide* access to our school's network through Microsoft 365;
- Staff access to the schools' management information system is controlled through a separate password for data security purposes;
- All pupils have access to student areas and the internet through year group log ins.
- Makes clear that no one should log on as another user and makes clear that pupils should never be allowed to log-on or use teacher and staff logins as these have far less security restrictions and inappropriate use could damage files or the network;
- Has set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas;
- Requires all users to always log off when they have finished working or are leaving the computer unattended;
- Where a user finds a logged-on machine, we require them to always log-off and then log-on again using their approved log on details.
- Requests that teachers and pupils do not switch the computers off during the day unless they are unlikely to be used again that day or have completely crashed. We request that they DO switch the computers off at the end of the day.
- Has set-up the network so that users cannot download executable files / programmes.
- Has blocked access to music/media download or shopping sites – except those approved for educational purposes;
- Makes clear that staff are responsible for ensuring that all equipment that goes home has the anti-virus and spyware software maintained up-to-date and the school provides them with a solution to do so;
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used solely to support their professional responsibilities and that they notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- Makes clear that staff accessing LA systems do so in accordance with any Corporate policies; e.g. finance system, Personnel system etc.
- Maintains equipment to ensure Health and Safety is followed; e.g. projector filters cleaned by site manager / TA; equipment installed and checked by approved Suppliers / LA electrical engineers
- Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems; e.g. technical support or MIS Support, our Local Authority Attendance Officers accessing attendance data on specific children, parents using a secure portal to access information on their child
- Provides pupils and staff with access to content and resources through the approved Learning Platform which staff and pupils access using their username and password (their USO username and password);

- Makes clear responsibilities for the daily back up of MIS and finance systems and other important files;
- Has a clear disaster recovery system in place for critical data that includes a secure, remote back up of critical data, that complies with external Audit's requirements;
- Ensures that all pupil level data or personal data sent over the Internet is encrypted or only sent within the approved secure system in our LA.
- Follows ISP advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network;
- Our wireless network has been secured to industry standard Enterprise security level /appropriate standards suitable for educational use;
- All computer equipment is installed professionally and meets health and safety standards;
- Interactive whiteboards are maintained so that the quality of presentation remains high;
- Reviews the school ICT systems regularly regarding health and safety and security.

Password policy

- This school makes it clear that staff must always keep their password private, must not share it with others and must not leave it where others can find it. If a password is compromised the school should be notified immediately.
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password private.
- We require staff to use STRONG passwords.
- Supply teachers have their own password which should only allow access to the Curriculum folder

E-mail

This school

- Provides staff and governors with an email account for their professional use, and makes clear personal email should be through a separate account;
- Will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.
- Will ensure that email accounts are maintained and up to date
- Reports messages relating to or in support of illegal activities to the relevant Authority and if necessary to the Police.
- Knows that spam, phishing and virus attachments can make e mails dangerous. We use a number LA provided technologies to help protect users and systems in the school, including desktop anti-virus product, plus direct email filtering for viruses, Trojans, pornography, phishing and inappropriate language. , Finally, and in support of these Cambridgeshire ICT services filtering, monitors and protects our Internet access to the World Wide Web.

Pupils:

- Pupils are introduced to and use e-mail as part of the ICT/Computing scheme of work.
- Pupils are taught about the safety and 'netiquette' of using e-mail both in school and at home i.e. they are taught:

- not to give out their e-mail address unless it is part of a school managed project or to someone they know and trust and is approved by their teacher or parent/carer;
- that an e-mail is a form of publishing where the message should be clear, short and concise;
- that any e-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper;
- they must not reveal private details of themselves or others in e-mail, such as address, telephone number, etc.;
- to 'Stop and Think Before They Click' and not open attachments unless sure the source is safe;
- that they should think carefully before sending any attachments;
- embedding adverts is not allowed;
- that they must immediately tell a teacher / responsible adult if they receive an e-mail which makes them feel uncomfortable, is offensive or bullying in nature;
- not to respond to malicious or threatening messages;
- not to delete malicious of threatening e-mails, but to keep them as evidence of bullying;
- not to arrange to meet anyone they meet through e-mail without having discussed with an adult and taking a responsible adult with them;
- that forwarding 'chain' e-mail letters is not permitted.

- Pupils sign the school Agreement Form to say they have read and understood the e-safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

Staff:

- Staff only use e-mail systems for professional purposes
- Access in school to external personal e-mail accounts may be blocked
- Staff know that e-mail sent to an external organisation must be written carefully, (and may require authorisation), in the same way as a letter written on school headed paper. That it should follow the school 'house-style':
  - The sending of multiple or large attachments should be limited, and may also be restricted by the provider of the service being used;
  - The sending of chain letters is not permitted;
  - Embedding adverts is not allowed;

- All staff sign acceptable use agreement, including e-mail and we explain how any inappropriate use will be dealt with.

School website

- The Headteacher take overall responsibility to ensure that the website content is accurate, and the quality of presentation is maintained;
- The Headteachers and the website manager are authorised to upload information to the website. Teachers are authorised to upload information and photos to their class pages.
- The school web site complies with the statutory DfE guidelines for publications;

- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status
- The point of contact on the website is the school address, telephone number and the office@bassingbourn.cambs.sch.uk school email contact address
- Teacher's work and class email details are published but home information or personal non-school e-mail identities will not be published
- Photographs published on the web do not have full names attached
- We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website
- Pupils in photos published must have a signed photo permission slip from parents
- We do not use embedded geodata in respect of stored images

Cloud Environments

- Uploading of information on the school's online learning space is shared between different staff members according to their responsibilities e.g. all class teachers upload information in their class areas and pupils upload to their own approved areas using accounts provided by the school.
- Photographs and videos are uploaded to either the school's online environment or approved accounts and will only be accessible by members of the school teaching staff and or the individual pupil.
- In school, pupils are only able to upload and publish within school approved 'Cloud' systems. From home, pupils and parents/guardians will be able to access the pupils' approved OneDrive accounts with authentication.

Social networking

- Teachers are instructed not to run social network spaces for student use on a personal basis or to open their own spaces to their students, but to use the schools' preferred system for such communications

School staff will ensure that in private use:

- No reference must be made in social media to students / pupils, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions must not be attributed to Bassingbourn Community Primary School or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

All members of our school community (staff /parents / governors) are informed that photos / videos of events must not be posted on social media without the permission of the Headteacher. Since 2018 photos and videos have not been permitted to be taken, by parents, at school events.

Video Conferencing

Bassingbourn Community Primary School

- Only uses supported services for video conferencing activity;
- Only uses approved or checked webcam sites;

CCTV

- We have CCTV in the school as part of our site surveillance for staff and student safety and for child protection purposes. We will not reveal any recordings (*retained by the Support Provider for 28 days*), without permission except where disclosed to the Police as part of a criminal investigation.

Recording Equipment

- We use recording equipment on occasions as a tool to share best teaching practice. We do not reveal any such recordings outside of the staff and will not use for any other purposes.

Responsibilities of Staff / Data Processors

All staff are responsible for:

1. Checking that any information that they provide to the School in connection with their employment is accurate and up to date.
2. Informing the School of any changes to information that they have provided, e.g. change of address, either at the time of appointment or subsequently. The School cannot be held responsible for any errors unless the staff member has informed the School of such changes.
3. Handling all personal data (e.g. pupil attainment data) with reference to this policy. Where data is requested the purpose of that information is stated and ensure that the information gathered is accurate.
4. Teacher Trainees / Parent Helpers / Governors may be provided with less information than school staff but are still required to adhere to this policy and those associated with it.

Data Security

All Data Processors must follow the Acceptable Use Policy (appendix to this document) and take note that:

1. All personal data that they hold is kept securely and should not be left in public areas where there is general access.
2. Personal information is not disclosed either orally or in writing or via Web pages or by any other means, accidentally or otherwise, to any unauthorised third party.
3. Personal information that individuals would expect to be treated as private or confidential (whether legally classified as sensitive personal data or not) is treated accordingly.
4. All portable electronic devices used for storing personal data on school business (including privately owned equipment) should be kept as securely as possible on and off school premises.

Staff should note that unauthorised disclosure will usually be a disciplinary matter and may be considered gross misconduct in some cases.

Personal information must:

1. Be kept in a filing cabinet, drawer, or safe in a secure office, or;

2. If it is computerised/electronic, be password protected both on a local hard drive and on a network drive that is regularly backed up. If it is sensitive personal data, strong passwords should be used, i.e. at least eight characters long and containing a mixture of letters/symbols/numbers. Passwords should be changed regularly and different passwords used for separate systems and devices. Laptops taken off site must be encrypted.
3. If a copy is kept on a usb memory stick or other portable/removable storage media, that media must be password protected, as above, and fully encrypted and/or kept in a secure filing cabinet, drawer, or safe. This is particularly important if they are taken from school premises.

Sharing Data
The school holds information on pupils to support their teaching and learning, to monitor and report on their progress, to provide appropriate pastoral care, and to assess how well the school is doing. This information includes contact details, national curriculum assessment results, attendance information, characteristics such as ethnic group, special educational needs and any relevant medical information. From time-to-time schools are required to pass on some of this data to LAs, the DfE and to agencies that are prescribed by law, such as Ofsted.

When considering sharing personal data, staff are responsible for making sure they are allowed to share it; and ensuring that adequate security (considering the nature of the information) is in place to protect it.

Rights to Access Information
All staff, parents and other users are entitled to:

1. Know what information the School holds and processes about them or their child and why.
2. Know how to gain access to it.
3. Know how to keep it up to date.
4. Know what the School is doing to comply with its obligations under the 2018 Regulation.

The School will, upon request, provide all staff and parents and other relevant users with a statement regarding the personal data held about them. This will state all the types of data the School holds and processes about them, and the reasons for which they are processed.

All staff, parents and other users have a right under the 2018 Regulation to access certain personal data being kept about them or their child either on computer or in certain files. Any person who wishes to exercise this right should make a request in writing and submit it to the Headteacher. The School will ask to see evidence of identity, such as a passport or driving licence, before disclosure of information.

The School aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 30 days, as required by the 2018 Regulation

Other Policies

This policy is to be read alongside our Data Retention Policy, Breach of Data Protection Policy, CCTV policy, Privacy Notices, Subject Access Request policy and Information Asset Register.

Management Information System access and Data transfer

Strategic and operational practices

At this school:

- The Head Teacher is the Senior Information Risk Officer (SIRO) and asset owner.
- We ensure staff know who to report any incidents where data protection may have been compromised.
- All staff are DBS checked, and records are held in one central record
- We ensure ALL the following school stakeholders sign an Acceptable Use Agreement form. We have a system, so we know who has signed.
    - staff,
    - governors,
    - pupils
    - parents

  This makes clear staffs' responsibilities regarding data security, passwords and access.
- We follow LA guidelines for the transfer of any data, such as MIS data or reports of children, to professionals working in the Local Authority or their partners in Children's Services / Family Services, Health, Welfare and Social Services.
- We require that any Protect and Restricted material must be encrypted if the material is to be removed from the school and limit such data removal. / We have an approved remote access solution so staff can access sensitive and other data from home. Memory sticks must be password protected.
- School staff with access to setting-up usernames and passwords for email, network access and Learning Platform access are working within the approved system and follow the security processes required by those systems.
- We ask staff to undertaken at least annual housekeeping to review, remove and destroy any digital materials and documents which need no longer be stored.

Technical Solutions

- Staff have secure area(s) on the network to store sensitive documents or photographs - My documents on their personal log in.
- We require staff to log-out of systems when leaving their computer but also enforce lock-out after 10 minutes idle time.
- We use encrypted flash drives if any member of staff has to take any sensitive information off site.
- We use the DfE S2S site to securely transfer CTF pupil data files to other schools.
- We use S2S system to transfer admissions data.
- We store any Protect and Restricted written material in lockable storage cabinets in a lockable storage area.
- All servers are in lockable locations and managed by DBS-checked staff.
- BCPS has cloud backup for some data and a networked backup for onsite servers
- We use Irvine Knight for computing and ICT support
- We comply with equipment disposal policy by using an approved or recommended disposal company for disposal of equipment where any protected or restricted data has

been held and get a certificate of secure deletion for any server that once contained personal data.
- Portable equipment loaned by the school (for use by staff at home), where used for any protected data, is disposed of through the same procedure.
- Paper based sensitive information is shredded, using crosscut shredder.

6. Equipment and Digital Content

Personal mobile phones and mobile devices

- Mobile phones brought into school are entirely at the staff member, student's & parents' or visitors own risk. The School accepts no responsibility for the loss, theft or damage of any phone or handheld device brought into school.
  - Student mobile phones which are brought into school must be turned off (not placed on silent) and given into their class teacher to be stored. Staff members may use their phones during school break times in the staff room. Mobile internet (such as 4g and 5g) should be disabled. All visitors and staff members are requested to leave their phones in a locker in the staff room during teaching time.
  - The recording, taking and sharing of images, video and audio on any mobile phone is to be avoided; except where it has been explicitly agreed otherwise by the Headteacher. Such authorised use is to be monitored and recorded. All mobile phone use is to be open to scrutiny and the Headteacher is to be able to withdraw or restrict authorisation for use at any time if it is to be deemed necessary.
- The School reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying. Staff mobiles or handheld devices may be searched at any time as part of routine monitoring.
  - Where parents or students need to contact each other during the school day, they should do so only through the School's telephone. Staff may use their phones during break times in the staff room or main office.
- Mobile phones and personally owned devices are not permitted to be used outside the staff room or main office unless they are being used as verification to access Office 365 online for a school account.
  - The Bluetooth or similar function of a mobile phone should be always switched off and not be used to send images or files to other mobile phones.

Students' use of personal devices

  - The School strongly advises that student mobile phones should not be brought into school.
- The School accepts that there may be circumstances in which a parent wishes their child to have a mobile phone for their own safety.
  - If a student breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents or carers in accordance with the school policy.
  - If a student needs to contact his or her parents or carers, they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.
- Students should protect their phone numbers by only giving them to trusted friends and family members. Students will be instructed in safe and appropriate use of mobile

phones and personally owned devices and will be made aware of boundaries and consequences.

Staff use of personal devices

- Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity.
- If members of staff have an educational reason to allow children to use mobile phones or a personally owned device as part of an educational activity, then it will only take place when approved by the senior leadership team.
- Staff should not use personally owned devices, such as mobile phones or cameras, to take photos or videos of students and will only use work-provided equipment for this purpose.
    - In an emergency where a staff member doesn't have access to a school-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes
- If a member of staff breaches the school policy, then disciplinary action may be taken.

Digital images and video
In this school:

- We gain parental / carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter / son joins the school;
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials / DVDs;
- Staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones / personal equipment for taking pictures of pupils;
- If specific pupil photos (not group photos) are used on the school web site, in the prospectus or in other high-profile publications the school will obtain individual parental or pupil permission for its long-term use
- Pupils are taught about how images can be manipulated in their e-safety education programme and taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their ICT scheme of work;
- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identify of others and their location, such as house number, street name or school. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

Asset disposal

Details of all school-owned hardware will be recorded in a hardware inventory. Details of all school-owned software will be recorded in a software inventory.

All redundant equipment will be disposed of through an authorised agency. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data. All redundant equipment that may have held personal data will have the storage media forensically wiped. Alternatively, if the storage media has failed, it will be physically destroyed. The school will only use authorised companies who will supply a written guarantee that this will happen. Disposal of any equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2013. Further information can be found on the Environment Agency website.

Disposal of any equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website.

Appendix 1 – Acceptable Use for Data Processors (adult)

A: Use of school based equipment and services

Access to school equipment, the school network and the internet

- I will access the internet and other ICT systems using an individual username and password, which I will keep secure. I will ensure that I log out after each session and never allow other users to access the internet through my username and password. I will report any breach of security to the e-safety coordinator/Headteacher.
- I will not search for, download, upload or forward any content that is illegal or that could be considered an offence by another user. If I encounter any such material I will report it immediately to the e-safety coordinator/ Headteacher. I will not download or install any software from the internet or from any other media which may compromise the school network or information situated on it.
- I will not attempt to bypass any filtering and/or security systems put in place by the school. If I suspect a computer or system has been damaged or affected by a virus or other malware, I will report this to the e-safety coordinator.
- I will seek written consent from the e-safety coordinator/ Headteacher prior to the use of any new technologies (hardware, software, cloud-based services) within school.
- I understand that my files, communications and internet activity may be monitored.

Creation, storage and security of digital content

- I will take reasonable precautions to ensure that any devices (laptops, tablets, cameras, removable media or phones) are stored in a secure manner when taken off site (car / home/ other location). Devices will not be stored in a car unattended or left in sight when not in use, e.g. by an open window. I will ensure that any personal or sensitive information taken off site will be situated on a school-owned device with appropriate technical controls such as encryption / password protection. If using my own device at home to view data, I will ensure that it is encrypted / password protected.
- I will use only school-provided portable storage (USB sticks, SD cards, portable hard drives etc) with encryption unless permission has been granted by the e-safety coordinator / Headteacher.
- I will demonstrate professional, safe and responsible behaviour when creating, using and storing digital images, video and sound within school. I will model safe and responsible behaviour in the creation and publishing of online content.
- I will use only school equipment to create digital images, video and sound unless prior permission is granted by the e-safety coordinator / Headteacher.
- I will ensure that I am familiar with the current permission status of pupils (see Parental Consent Form for Digital Images and Video). A summary of all permissions are circulated to all staff and available from the office. If additional permission is needed, e.g. for a surname in the press or for a medical form, then I will discuss this with the e-safety coordinator and further written permission will be sought.
- I will ensure that I am familiar with the current Data Protection Policy. I will manage my digital files in accordance with this and I will make myself familiar with procedures in case of a breach of data security.
- I will not leave my computer unattended whilst working on screen; instead I will press CTL/ALT/DLT to lock the screen.
- I will only store / retain data files in line with the Data Retention Policy and will be responsible for deleting files which are no longer required.

School email and calendars

- I will use my school email address for all school-related correspondence. I understand that any use of the school email system will be monitored and checked. I will not use my private email account for any school-related business. Email is the main method of communication for all school matters and I will check my e-mail regularly and respond in a timely manner (in normal working hours) to communications that require my attention.
- I will take care in opening any attachments sent by email. I will only open emails and associated attachments from trusted senders.

- Communication between staff or members of the wider school community should be professional and related to school matters only. Emails sent to external organisations will be written carefully and if necessary authorised before sending to protect members of staff. It is best practice when emailing parents and/or carers to add all intended recipients to the BCC address field. This ensures that parents' personal email addresses are not visible to others.
- To avoid the misrepresentation of others I will not make changes to someone else's e-mail and then pass it on without making it clear where changes have been made.
- I will take great care when forwarding messages to ensure that no confidential or sensitive material (e.g. other's email addresses) are attached
- The school calendar on Outlook is the central calendar for all school matters. I will check it regularly and take events into account when planning lessons and visits etc. I will add events and appointments to the calendar as necessary. I will also regularly check the school calendar.

Learning and teaching

- In line with every child's legal entitlement I will ensure I teach / model an age-appropriate e-safety curriculum.
- I will always support and promote the school e-safety policy. I will model safe and responsible behaviour to pupils when using ICT to support learning and teaching.
- I will ensure that I am aware of my 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.
- I understand the importance of respecting and acknowledging copyright of materials found on the internet and will always model best practice in the creation of my own resources.
- I will ensure that all online services and software that I use as part of my teaching are appropriate and are used in line with current guidance.
- I agree to adhere by the school's Prevent guidelines and action plan.

B: Personal equipment and services

Social media and messaging

- I will not talk about my professional role in any capacity when using personal social media. I will not use social media tools to communicate with current or former pupils under the age of 18 nor to communicate with parents in a professional capacity. I will be mindful of potential conflicts of interest where a parent or carer of a child at the school is also a friend. I will set and maintain my profile on social networking sites to maximum privacy. I will not access social networking sites for personal use during school hours.
- If I experience any derogatory or slanderous comments relating to the school, colleagues or my professional status, I will take screenshots for evidence and bring this to the attention of the e-safety coordinator or Headteacher.
- Use of school equipment or e-mail accounts for personal financial gain, gambling, political purposes or advertising is forbidden. However, nothing in this paragraph is intended to restrict members of staff conducting any trade union or professional association using school computers or e-mail accounts, outside of teaching hours.

Personal mobile phones and other devices

- I will not bring my mobile into teaching spaces unless with the overt permission of the Headteacher. If permitted, I will ensure that my mobile phone and any other personally owned device is switched off or switched to silent mode during teaching hours and used only in emergencies.
- I will not contact any parents or pupils on my personally owned device unless in an emergency. If a pupil or parent contacts me using my personal device I will inform the Headteacher as soon as possible. On educational visits my personal mobile phone may be used to contact the school.

- I will not use any personally owned mobile device to take images, video or sound recordings in school without the overt, written permission of the Headteacher (e.g. twitter feed)
- I will seek permission from the e-safety coordinator / Headteacher if I need to synchronise any school email account with a personally owned device. If permission is granted, then I will ensure that the device has the appropriate technical controls such as encryption / password protection.

Exceptional circumstances:
Due to unforeseen circumstances (e.g. school closures, distance learning and or isolated classes) it may become necessary and even vital for staff to have a mobile phone accessible in the classroom. Furthermore, the use of their phone may be required for the following reasons (not a definitive list and can be altered by the Head Teacher to restrict or add additional provisions):

- To ring SLT in an emergency from within an isolated provision;
- To receive calls from SLT whilst in an isolated provision;
- To record educational based videos in school to support students' learning. In this situation, no children should be visible nor should their names be used. Recording should only take place with two adults present.
- All mobile phones will need to be kept out of sight within a drawer or bag unless being used in accordance with this policy amendment, but they should remain accessible in case of emergencies.
- Mobile phones should not be used for personal reasons during class time whilst the children are present.

In the case of Exceptional Circumstances being required, an email will be sent out by a designated member of staff, requiring all staff members affected to read the amended policy entry and to respond by email to confirm that they have read it and agree to follow the new working practises.

C: Maintaining Professional Standards and Boundaries

Staff should always maintain appropriate professional boundaries, avoid behaviour which could be misinterpreted by others and report any such incident to a senior manager. This is as relevant in the online world as it is in the classroom; staff engaging with pupils and / or parents online (via email for example) have a responsibility to always model safe practice.

If any safeguarding concerns are raised through online contact via pupil posts or through communications with parents via email, then a referral should be made as soon as possible to a designated member of staff. If you are offsite, please contact a designated member of SLT.

D: Use of technology for online/ virtual teaching

- Wherever possible, staff should use school devices and contact pupils only via approved methods as set out below:
    - Parent email account via the class email or teacher's school email account;
- Staff engaging in online learning should display the same standards of dress and conduct that they would in the real world; they should also role model this to pupils and parents.
- Things to consider (especially if delivering live lessons):
    - Think about the background; photos, artwork, identifying features, mirrors – ideally the backing should be blurred;
    - Staff and pupils should be in living / communal areas – no bedrooms;
    - Staff and pupils should be fully dressed;
    - Filters at a child's home may be set at a threshold which is different to the school;
    - Resources / videos must be age appropriate – the child may not have support immediately to hand at home if they feel distressed or anxious about content;
- Staff members should:
    - Adhere to their establishment's policy;
    - Be fully dressed and dressed appropriately for their role;

    - Ensure that a senior member of staff is aware that the online lesson / meeting is taking place and for what purpose;
    - Avoid one to one situations – request that a parent is present in the room for the duration, or ask a colleague or member of SLT to join the session;
    - Only record a lesson or online meetings with a pupil where this has been agreed with the head teacher or other senior staff member, and the pupil and their parent/carer have given explicit written consent to do so;
    - Be able to justify images of pupils in their possession;
- Staff members should not:
    - Contact pupils outside the operating times defined by senior leaders;
    - Take or record images of pupils for their personal use;
    - Record virtual lessons or meetings using personal equipment (unless agreed and risk assessed by senior staff);
    - Engage online while children are in a state of undress or semi-undress;

It is the responsibility of the staff member to act as a moderator; raise any issues of suitability (of dress, setting, behaviour) with the child and / or parent immediately and end the online interaction if necessary. Recording lessons does not prevent abuse. If staff wish to record the lesson they are teaching, consideration should be given to data protection issues; e.g., whether parental / pupil consent is needed and retention / storage. If a staff member believes that a child or parent is recording the interaction, the lesson should be ended or that child should be logged out immediately. Staff, parent and pupil AUPs should clearly state the standards of conduct required.

If staff need to contact a pupil or parent by phone and do not have access to a work phone, they should discuss this with a senior member of staff and, if there is no alternative, always use 'caller withheld' to ensure the pupil / parent is not able to identify the staff member's personal contact details.

Data Processors found to be in breach of these rules may face disciplinary action in line with the school's disciplinary procedures.

Full name (Please print):

_____

Signed: _____

Date: _____

Appendix 2 – KS2 Acceptable Use

Bassingbourn Primary School
Pupil KS2 Rules for Responsible Internet Use

These rules will keep me safe and help me to be fair to others.

- I will ask permission to go online.
- I will only edit or delete my own files and not look at, or change, other people's files without their permission.
- I will not bring files into school without permission or upload inappropriate material to my workspace.
- I am aware that some websites and social networks have age restrictions, and I should respect this by not using them without permission.
- I will not attempt to visit Internet sites that I know to be banned by the school.
- I will only e-mail people I know, or a responsible adult has approved.
- The messages I send, or information I upload, will always be polite and sensible.
- I will not open an attachment, or download a file, unless I know and trust the person who has sent it.
- I will not give my home address, phone number, school address or telephone number, send a photograph or video, or give any other personal information that could be used to identify me, my family, my school or my friends, unless a trusted adult has given permission.
- I will never arrange to meet someone I have only ever previously met on the Internet, unless my parent/carer has given me permission and I take a responsible adult with me.
- If I see anything I am unhappy with or receive a message I do not like, I will not respond to it, but I will show a teacher / responsible adult.
- If I need to bring a phone to school, I will pass hand it in as soon as I enter my class.
- I will not use my mobile phone on school grounds, unless I have been given permission to do so by a member of staff. If I do use my mobile phone without permission, I understand that it may be confiscated.
- If I use material that is the work of others in my work, I will state where I found the information.
- I will use a range of passwords, keep all passwords safe and never share account details with others.

I have read and understand these rules and agree to them.

Child's name: _____ Parent's signature: _____

Child's signature: _____ Date: _____

The school accepts no responsibility for inappropriate use of the Internet outside school, even when children are researching a school-based subject.

Think before you click

S

I will only use the Internet and email with an adult's permission

A

I will only click on icons and links when I know they are safe

F

I will only send friendly and polite messages

E

If I see something I don't like on a screen, I will always tell an adult