Bridge Junior School

E-Safety Policy

2022-23

Contents

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 Bridge Junior School with respect to the use of ICT-based technologies.
- Safeguard and protect the children and staff of Bridge Junior 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 pupils.

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

Content: being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.

Contact: being subjected to harmful online interaction with other users; for example: 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; for example, 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.

Scope

This policy applies to all members of our school community (including staff, pupils, volunteers, parents/carers, visitors, community users, governors) who have access to and are users of school ICT systems, both in and out of school.

The Education and Inspections Act 2006 empowers headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data.

The school will deal with such incidents within this policy and associated Behaviour, Anti-bullying and Child Protection & Safeguarding policies and will, where known, inform parents /carers of incidents of inappropriate e-safety behaviour that take place out of school.

Roles and Responsibilities

Headteacher

- To take overall responsibility for e-safety provision
- To take overall responsibility for data and data security
- 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 receive regular monitoring reports from the Computing Coordinator
- To ensure that there is a system in place to monitor and support staff who carry out internal
- e-safety procedures (e.g. IT technician)

Computing Coordinator with the Designated Safeguarding Lead

- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies and 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's IT technician
- To communicate regularly with SLT and the designated safeguarding governor to discuss current issues, review incident logs and filtering control logs
- To ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident
- To ensure that an e-safety incident log is kept up to date
- Facilitates training and advice for all staff
- Liaises with the Local Authority and relevant agencies
- 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

- To ensure that the school follows all current e-safety advice to keep the children and staff safe
- To approve the E-Safety Policy and review the effectiveness of the policy
- To support the school in encouraging parents and the wider community to become engaged in e-safety activities

Computing Coordinator

- To oversee the delivery of the e-safety element of the Computing curriculum
- To liaise with the designated safeguarding lead regularly

ICT technician

- To report any e-safety related issues that arises, to the Computing Coordinator and or the designated safeguarding lead
- To ensure that users may only access the school's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed
- To ensure that provision exists for misuse detection and malicious attack e.g. keeping virus protection up to date)
- To ensure the security of the school ICT system
- To ensure that access controls / encryption exist to protect personal and sensitive information held on school-owned devices
- the school's policy on web filtering is applied and updated on a regular basis
- Keeps up to date with the school's E-safety Policy and technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- That the use of the network (including remote access) and email is regularly monitored in order that any misuse / attempted misuse can be reported to the designated person (In the first instance the Headteacher) for investigation
- To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster

- To keep up-to-date documentation of 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

All staff

- 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 (AUP)
- To be aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices
- To report any suspected misuse or problem to the designated safeguarding lead
- 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
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- To understand the importance of reporting abuse, misuse or access to inappropriate materials
- To know what action to take if they or someone they know feels worried or vulnerable when using online technology
- To know and understand school policy on the digital technologies including but not limited to cameras, iPads and mobile phones
- To know and understand school policy on the taking / use of images and on cyber-bullying
- To understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school

Parents/carers

- To support the school in promoting e-safety and endorse the Parents' Acceptable Use Agreement which includes the pupils' use of the Internet and the school's use of photographic and video images
- To read, understand and promote the school Pupil Acceptable Use Agreement with their children
- To consult with the school if they have any concerns about their children's use of technology

External visitors/groups

- Any external individual / organisation will sign an Acceptable Use Policy prior to using any equipment or the Internet within school

Communication

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

- Policy to be posted on the school website
- 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

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. Sanctions available include:

- Sanctions under the school Behaviour Policy
- Interview with class teacher, year group leaders, senior leaders or Headteacher
- Informing parents/carers
- Removal of Internet or computer access for a period
- Referral to LA / Police

Our Computing 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 and Anti-Cyberbullying Policy. Complaints related to child protection are dealt with in accordance with school and LA child protection procedures.

Review and Monitoring

The E-safety Policy is not a standalone policy and should be read in conjunction with (but not limited to) our curriculum policies, Safeguarding & Child Protection policy, Anti-Bullying policy and Behaviour policy.

The school Computing Coordinator and designated safeguarding lead will be responsible for document ownership, review and updates.

The E-safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school.

2. Education and Curriculum

Pupil e-safety curriculum

This school follows a progressive e-safety education programme as part of the Computing and RHE curriculum.

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
- Ensure there are trained staff to deal with e-safety issues when they arise and that staff who can support them
- 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

Our school will offer advice, guidance and training for parents where appropriate including:

- ✓ Information leaflets; in school newsletters; on the school web site
- ✓ suggestions for safe Internet use at home
- ✓ provision of information about national support sites for parents

3. Expected Conduct and Incident management

Expected conduct

At Bridge Junior School, all users are responsible for using the school's ICT systems in accordance with their roles outlined in section 1.

All users will also be expected to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so, as well as recognising that this policy covers their actions outside of school.

All users, should also read this policy in line with all other school policies to ensure effective implementation across the school.

Incident Management

In our 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 need 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
- Support is actively sought from other agencies (as needed) in dealing with e-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 children 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

4. Managing the ICT infrastructure

Internet access, security (virus protection) and filtering

Benefits of using the Internet in education include:

- ✓ access to world-wide educational resources including museums and art galleries
- ✓ educational and cultural exchanges between pupils world-wide
- ✓ access to experts in many fields for pupils and staff
- ✓ professional development for staff through access to national developments, educational materials and effective curriculum practice
- ✓ collaboration across support services and professional associations
- ✓ improved access to technical support including remote management of networks and automatic system updates
- ✓ exchange of curriculum and administration data with the Local Authority and DfE; access to learning wherever and whenever convenient.

How can Internet Use Enhance Learning?

- The school Internet access will be designed specifically for pupil use and includes filtering appropriate to the age of pupils
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use
- Internet access will be planned to enrich and extend learning activities
- Staff should guide pupils in on-line activities that will support learning outcomes planned for the pupils' age and maturity
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Authorised Internet Access

- The school will maintain a current record of all staff and pupils who are granted Internet & network access
- All staff must read and sign the 'Acceptable Use Agreement' before using any school ICT resource
- Parents will be informed that pupils will be provided with supervised Internet access
- Parents will be asked to sign and return a consent form for pupil access.

World Wide Web

- If staff or pupils discover unsuitable sites, the URL (address), time, content must be reported to the Computing Coordinator or IT technician
- School will ensure that the use of Internet derived materials by pupils and staff complies with copyright law
- Pupils should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy

Filtering

- The school will work in partnership with the Local Authority and the Internet Service Provider to ensure filtering systems are as effective as possible

Password policy

- This school makes it clear that staff and pupils must always keep their password private, must not share it with others and must not leave it where others can find it
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password private.

E-mail

Our school;

- Provides staff with an email account for their professional use. Personal email should be through a separate account and not used for school business
- Does not publish personal e-mail addresses of pupils or staff on the school website
- Will contact the Police if one of our staff or pupils receives an email 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

School website

- The Headteacher takes overall responsibility to ensure that the website content is accurate, and the quality of presentation is maintained
- Uploading of information is restricted to our website authorisers
- 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 we use a general email contact address. Home information or individual email 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
- We expect teachers using' school approved blogs or wikis to password protect them and run from the school website

Social Media

Use of Twitter, other social networking and personal publishing

- The school will block/filter access to social networking sites
- News groups will be blocked unless a specific use is approved
- Pupils will be advised never to give out personal details of any kind which may identify them or their location
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils
- Pupils and parents will be advised on how to access and use the privacy settings on social media platforms

The school will take action if any of the following actions are committed by pupils or staff:

- Offensive language aimed the staff, school, parents, governors or others affiliated with the school
- Unsuitable comments or pictures posted on feeds
- Images or text which infringe upon copyright
- Comments that aim to undermine the school, staff, parents, governors or others affiliated with the school

Video Conferencing

- IP video conferencing should use the educational broadband network to ensure quality of service and security rather than the Internet
- Advice from the Computing Coordinator, ICT technician or Headteacher should be sought before making or answering a video conference call
- Video conferencing will be appropriately supervised for the pupils' age

CCTV

- We have CCTV in the school as part of our site surveillance for staff and student safety. We will not reveal any recordings (retained for a limited period), without permission except where disclosed to the Police as part of a criminal investigation.

5. Data security: Management Information System access and Data transfer

Storing date securely is covered within our data protection policy. Data Protection Personal data will be recorded, processed, transferred and made available according to the General Data Protection.
Regulation Act 2018 and the schools' GDPR Policy. Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly 'logged-off' at the end of any session in which they are using personal data
- Transfer data using encryption and secure password protected devices

General Data Protection Regulations/Data Protection Act 2018
This protects the rights and privacy of individual's data. To comply with the law, only necessary information about individuals must be collected. It must be used fairly, stored safely and securely and not disclosed to any third party unlawfully. Individuals have the right to access the data that is held on them except with data relating to safeguarding. The Act states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Not kept longer than necessary
- Processed in accordance with the data subject's rights
- Secure
- Transferred securely

6. Equipment and Digital Content

This section should be read in conjunction with the Social Media section

Personal mobile phones and mobile devices

- Mobile phones brought into school are entirely at the staff member, pupils & 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 to the office at the start of the school day. They may be collected at the end of the school day. The school must have a letter from the pupil's parents explaining why it is necessary for the pupil to bring the mobile into school. This will be kept in the pupil's individual file
- All visitors are requested to keep their phones on silent
- 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 (including but not limited to IPADs, tablets, watches) on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying
- Where parents or pupils 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 or lunchtimes, when pupils are not around. If a staff member is expecting a personal call, they may leave their phone with the school office to answer on their behalf or seek specific permissions to use their phone at other than their break times
- Mobile phones and personally owned devices will not be used in any way during lessons or formal school time. They should be switched off or silent at all times and stored securely (ideally not on their person)
- Mobile phones and personally owned mobile devices brought into school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally owned mobile phones or mobile devices
- Mobile phones and personally owned devices are not permitted to be used in certain areas within the school site, e.g.IT suite, toilets, hall etc

Digital images and video

In our 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
- 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
- The school blocks/filter access to social networking sites or news groups unless there is a specific approved educational purpose
- Pupils are taught about how images can be manipulated in their e-safety curriculum lessons and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their Computing 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.

Appendix 1

E-Safety - Possible teaching and learning activities

Activities	Key E-Safety issues	Relevant websites/Apps
Learning about cyberbullying	Pupils should be supervised. Relevant material should be used.	NSPCC THINK U KNOW Anti-Bullying Alliance
Using search engines to access information from a range of websites.	Parental consent should be sought. Pupils should be supervised. Pupils should be taught how search engines work. Integral to this is pupils fully understanding the procedure to follow should they come across any inappropriate material: screen off and hands up.	Web quests e.g. Google
Creating an Advert	Parental consent should be sought. Pupils should seek staff and pupils permission before filming them Pupils be taught about copyright	IMovie
Publishing pupils' work on school and other websites.	Pupil and parental consent should be sought prior to publication for websites other than school. Pupils' full names and other personal information should be omitted.	Bridge Junior Website
Publishing images including photographs of pupils.	Parental consent for publication of photographs should be sought. File names should not refer to the pupil by name.	Bridge Junior Website

Appendix 2

E-Safety Audit

This quick audit will help editing and rewriting the policy annually.

Has the school an E-Safety policy that complies with CFE guidance?	Y/N
Date of latest update:	
The policy was agreed by governors on:	
The policy is available for staff at:	
And for parents at:	
The E-safety lead/Designated Child Protection Leader is:	
Has E-Safety training been provided for both students and staff?	Y/N
Do all staff sign a Computing Acceptable Use Agreement on appointment?	Y/N
Do parents sign and return an agreement that their child will comply with the school E-Safety rules?	Y/N
Have school E-Safety rules been set for pupils?	Y/N
Are these rules displayed in all rooms with computers?	Y/N
Internet access is provided by an approved educational Internet service provider and complies with DfE requirements for safe and secure access.	Y/N
Is personal data collected, stored and used according to the principles of the Data Protection Act?	Y/N

Appendix 3

Responsible Computing Use Agreement

Pupil's Agreement

At Bridge Junior School, we use the school computers and internet connection for learning.
These rules will help us to be fair to others and keep everyone safe.

- ✓ I will behave and follow the school's SHINE rules when I am using a computer/device or accessing anything, including TEAMS.
- ✓
- ✓ I will always use what I have learned about e-safety to keep myself safe and will tell a teacher if something makes me worried or unhappy.
- ✓ I will only use school computing equipment for my school work and not to upset or bully other people or create a bad impression of my school.
- ✓ I will take responsibility for my own use of all computing equipment and will use it safely, responsibly and legally.
- ✓ I will not go on any unsuitable or illegal web sites on purpose e.g. rude images, violence and racism. If I go on any by mistake, I will tell a teacher or my parents (if I am learning from home) straight away.
- ✓ I will tell a teacher if I can see a website that is inappropriate.
- ✓ I will look after school computing equipment and report any damage to a teacher straight away.
- ✓ I will not try to get past any security measures in place to protect the school network.
- ✓ I will only use the usernames and passwords I have been given and I will keep them secret.
- ✓ If I use Scratch to code at home, I know it is safer to use my class log in details for this.
- ✓ I will save only school work on the school network and will check with my teacher before printing.
- ✓ I will log off or shut down a computer when I have finished using it.
- ✓ I will not take part in any on-line internet chat groups.
- ✓ I understand that everything I do in school or when I'm learning (set by my teacher) from home is monitored and can be seen by my teacher and the Headteacher.
- ✓ I understand that my parents will be told if I am sharing anything that is unsafe or inappropriate.

I agree that I understand and will follow the rules above

Child's Name…… **Date……**

Child's Signature…… **Class……**

Parent's Consent for Internet Access

I have read and understand the school rules for responsible Computing and Internet use and give permission for my child (named above) to access the Internet.

I understand that the School will take all reasonable precautions to ensure pupils cannot access inappropriate materials.

I understand that the School cannot be held responsible for the nature or content of materials accessed through the Internet.

I agree that the School is not liable for any damages arising from the use of the Internet facilities.

Signature of Person with Parental Responsibility: ……..

Date ……

Appendix 4

Bridge Junior School **Acceptable Use: Staff Agreement form**

Staff with loaned laptops

1. I agree to back all my work on a regular basis. I also understand the school will not take any responsibility for their loss of work at any time.
2. I agree to use the Anti-Virus software that is installed on the laptop. I agree not to remove or replace it with another Anti-Virus application.
3. I agree that if I am having any technical issues with the laptop I will return to the school as soon as possible and discuss it with the IT team.
4. In the event of the laptop being stolen or damaged through my negligence, I am aware that I will be liable to pay the full cost associated with the results of my negligence.
5. I agree and accept that any computer or laptop loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue & Customs.
6. I agree to bring the laptop to school to make sure the laptop is up to date with windows security, Antivirus and any maintenance issues.
7. The laptop, and any accessories provided with it, remains the property of Bridge Junior School and is strictly for my use in delivering the curriculum.
8. I agree to not store images of the children on my laptop or mobile device for extended periods of time.

All Staff

9. I agree to only photograph or video children, whose parents have granted permission, solely for school use.
10. I strictly agree to use software that is licensed by the Headteacher of the School and installed by the IT technician.
11. I understand that I am responsible for my computer activity, internet or otherwise, and Bridge Junior School will not be responsible for any misuse.
12. I will only use the School's email / internet etc. for professional purposes or for uses deemed 'reasonable' by the Headteacher and Governing Body.
13. I will not browse, download or send material that could be considered offensive to colleagues.
14. I will report any accidental access to inappropriate materials to the appropriate line manager.
15. I will not download any software or resources from the internet that can compromise the network, or is not adequately licensed.
16. I understand that all internet usage is logged and this information could be made available to senior management on request.
17. I understand that failure to comply with the Usage Policy could lead to disciplinary action.
18. I agree to adhere to of Bridge Junior School policies regarding:
    - Acceptable use.
    - Health and safety.

Please note that these procedures are there to ENSURE your safety.

Children and online safety away from school

As above, all online lessons should be delivered by school staff in accordance with th
safeguarding and child protection, staff behaviour (code of conduct) and acceptable use of ICT policies.

The school will take account of guidance from DfE in relation to the planning and delivery of online learning when it is issued; as well as nationally recognised guidance including *guidance from the UK Safer Internet Centre on safe remote learning* and *London Grid for Learning on the use of videos and livestreaming*.

Staff will always use school/service owned technology and accounts for the delivery of remote lessons/tutorials. Where possible, applications that facilitate the recording of lessons will be used. School leaders will randomly sample recorded lessons in order to safeguard pupils/students and staff and to ensure that policies are being followed.

If staff need to deliver lessons/tutorials on a one-to-one basis or communicate with vulnerable children who are not attending school via video chat, they will speak to parents/carers before lessons commence and at the end of lessons before logging off.

The school will request and obtain written consent from parents/carers before staff communicate with children online.

It is important that all staff who interact with children, including online, continue to look out for signs that a child may be at risk, distressed for some reason or vulnerable in some other way; and report and record that following normal safeguarding procedures. All such concerns must be brought to the attention of a DSL and dealt with by a DSL as per the main policy in the normal way.

The school will ensure that online learning tools and systems are used in line with privacy and data protection/GDPR requirements.

Below are other issues that staff need to consider when delivering virtual lessons, especially where webcams are involved:

- Staff and children must wear suitable clothing, as should anyone else in the household.
- Any computers used should be in appropriate areas, for example, not in bedrooms; and the background should be blurred.
- The live class should be recorded so that if any issues were to arise, the video can be reviewed.
- Live classes should be kept to a reasonable length of time, or the streaming may prevent the family 'getting on' with their day.
- Language must be professional and appropriate, including that used by any family members in the background.
- Staff must only use platforms specified by senior managers and approved by the school's ICT manager/co-ordinator for communication with pupils/students.
- Staff should record the length, time, date and attendance of any sessions held.

The school recognises that school is a protective factor for children and young people and that the extraordinary circumstances created by the COVID-19 virus may well affect the mental health of some pupils/students and/or their parents/carers.

All staff will maintain as awareness of those issues in communications with children and their parents/carers including when setting expectations of pupils' work when they are at home.

Name: _____

Position: _____

Signature

I agree to abide by the above Acceptable Usage Policy.

Signature …….…….…… Date ……

Full Name ……..... (printed)

Job title . . . . . .

Laptop loanees only

Laptop Make: _____ Model Number: _____

Serial Number: _____

I have read and agree to adhere to the terms and conditions set out overleaf.

Authorised Signature (Head Teacher)

Is this member of staff temporary? NO / YES If yes, contract end date: ……..

I approve this email account / connection to the Internet.

Full Name ……..… (Print)

Signature ……..…….. Date ……

One copy is retained by member of staff | Second copy for school fill

Category:	Safeguarding/ Curriculum/E-safety
Purpose:	To set out the key principles expected of all members of the school community at Bridge Junior School with respect to the use of ICT-based technologies. To safeguard and protect the children and staff of Bridge Junior School.
Date ratified:	October 2022
Review Date:	*This policy will be reviewed annually. Any suggested amendments will be presented to the Governing Body for approval.* **October 2023**
Coordinator/s:	Headteacher/Computing Lead/IT Technician
Signed (& dated) by:	(Chair of Governors)