A Place to Flourish

"I have come that they may have life, and have it to the full" (John 10:10)

Online Safety Policy

Statutory Policy

Date of review/adoption	Autumn 2021
Date of next review	Autumn 2024
Notes	Reviewed March 2023

Signed … Jane Liddell* **… Chair of Governors**

Date ……01.11.21……

**Electronically signed and approved at Full Governing Board Meeting held on 01.11.21*

CONTENTS

BLUNDESTON CEVC PRIMARY SCHOOL
ONLINE SAFETY POLICY

1. Aims

At Blundeston CEVC Primary School, we recognise the wonderful learning opportunity provided by the online world and we want our children to be able to explore it safely and confidently. Online safety is a part of the curriculum and forms a part of the overarching **Safeguarding and Child Protection Policy**. Governors are responsible for ensuring that up-to-date safeguarding guidance and practices are embedded in school culture.

This policy aims to:

- Set out expectations for all members of the Blundeston school community's online behaviour, attitudes and activities and use of digital technology (including when devices are offline);
- Help all stakeholders to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of the school gates and school day, and regardless of device or platform;
- Facilitate the safe, responsible and respectful use of technology to support teaching & learning, increase attainment and prepare children and young people for the risks and opportunities of today's and tomorrow's digital world, to survive and thrive online;
- Help school staff working with children to understand their roles and responsibilities to work safely and responsibly with technology and the online world:
    - for the protection and benefit of the children and young people in their care, and
    - for their own protection, minimising misplaced or malicious allegations and to better understand their own standards and practice
    - for the benefit of the school, supporting the school ethos, aims and objectives, and protecting the reputation of the school and profession;
- Establish clear structures by which online misdemeanours will be treated, and procedures to follow where there are doubts or concerns (with reference to other school policies such as the Behaviour Policy and Anti-Bullying Policy).

2. Legislation and statutory responsibilities

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education and its advice for schools on preventing and tackling bullying. It also refers to the Department's guidance on protecting children from radicalisation (the Prevent Duty).

It reflects existing legislation, including but not limited to the Education Act 2002, the Education and Inspections Act 2006, Equality Act 2010 and Defamation Act 2013. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyberbullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so. The policy also takes into account the National Curriculum computing programmes of study

3. Roles and responsibilities

(N.B. All lists are not intended to be exhaustive).

3.1 The Governing Board

Key responsibilities:

- Have an awareness of online threats, risks and trends in technology use and internet use;
- Support and critically challenge the school in implementing effective online safety policy, procedure and practice;
- Ensure the school provides an appropriate level of filtering and monitoring which safeguards young people from risky online content and contact;
- Receive and act upon regular online safety reports from senior leaders;
- Ensure children are taught about online safety through teaching and learning opportunities as part of a broad and balanced curriculum;
- Provide all staff with appropriate online safety training;
- Appoint a named governor as the Online Safety Governor.

3.2 Online Safety Governor

Key responsibilities:

- Ensure that up-to-date online safety guidance and practices are embedded in school culture;
- Meet annually with the Online Safety Leads to discuss policy, procedures and curriculum;
- Monitor online safety incidents logged on CPOMS;
- Ensure that the level of filtering is appropriate;
- Attend relevant training on online safety.

3.3 Designated Safeguarding Lead

The Headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school. As the DSL, the Headteacher also takes lead responsibility for online safety in school.

Key responsibilities:

- Working with the Online Safety Leads and other staff, as necessary, to address any online safety issues or incidents;
- Ensuring that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy;
- Ensuring that any incidents of cyberbullying are logged and dealt with appropriately in line with the school's Behaviour Policy;
- Updating and delivering staff training on online safety;
- Liaising with the local authority, other agencies and/or external services if necessary in line with 'Working together to safeguard children';
- Ensure governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety.

3.4 Online Safety Leads

The Online Safety Leads are responsible for overseeing the implementation of agreed policies, procedures, curriculum requirements and staff training.

Key responsibilities:

- Working alongside the DSL in taking day-to-day responsibility for online safety issues and have a leading role in establishing and reviewing this policy and associated documents (see Appendices);
- Providing regular reports on online safety in school to the Headteacher and/or governing board;
- Receiving regular updates in online safety issues and legislations and being aware of national, local and school trends;
- Ensuring training is up-to-date and attending refresher courses on online safety;
- Ensuring that all staff are aware of the procedures that need to be followed in the event of an online safety incident;
- Receiving alerts via CPOMS about any online safety incidents;
- Liaising with the schools' technical, nurture and support staff as appropriate;
- Leading the pupil Digital Leaders;
- Meeting annually with the Online Safety Governor to discuss and review policy, procedures and curriculum;
- Overseeing and discussing appropriate filtering and monitoring with governors and ensure that staff are aware;
- Ensuring a GDPR-compliant framework for storing data.

3.5 IT Technician

Key responsibilities:

As listed in 'Staff' section below, plus:

- Ensuring that the school meets required online safety technical requirements and any online safety policy/guidance that may apply;
- Working with the Online Safety Leads to ensure that school systems and networks reflect school policy;
- Applying and updating filtering systems (Smoothwall) when required, ensuring its implementation is not the sole responsibility of any single person - the school has a login and instructions are available to all staff. Overall, the filtering system is supported and provided by Suffolk County Council;
- Ensuring the filtering is set to the correct level for staff and pupils, in the initial setup of a network, stand-alone PC, staff/pupil laptops and iPads;
- Ensuring all internet activity in school is routed via SCC's proxy server (SCC networks staff monitor this activity and can recall it if required) - the school can also provide reports on pupil activity;
- Ensuring there is appropriate and up-to-date anti-virus software and anti-spyware on the network, stand-alone PCs and staff/pupil laptops and that this is reviewed and updated on a regular basis (Trend Micro);
- Maintain up-to-date documentation of the school's online security and technical procedures;

- Manage the school's systems, networks and devices, according to a strict password policy, with systems in place for detection of misuse and malicious attack, with adequate protection, encryption and backup for data, including disaster recovery plans, and auditable access controls.

3.6 Staff

Key responsibilities:

- Understand that online safety is a core part of safeguarding; as such it is everyone's responsibility – never assume or think that someone else will pick it up;
- Know who the Designated Safeguarding Lead/Deputy DSLs and Online Safety Leads are;
- Read Part 1, Annex A and Annex C of Keeping Children Safe in Education (whilst Part 1 is statutory for all staff, Annex A for SLT and those working directly with children, it is good practice for all staff to read all three sections);
- Read and follow this policy in conjunction with the school's main Safeguarding and Child Protection Policy;
- Record online safety incidents in the same way as any safeguarding incident and report in accordance with school procedures;
- Understand that safeguarding is often referred to as a jigsaw puzzle – you may have discovered the missing piece so do not keep anything to yourself;
- Sign and follow the Staff Acceptable Use of Technology Policy (see Appendices);
- Notify the DSL/Online Safety Leads if the policy does not reflect practice in the school and follow escalation procedures if concerns are not promptly acted upon, using the Whistleblowing Policy if appropriate;
- Identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum, supporting subject leaders, and making the most of unexpected learning opportunities (which have a unique value for pupils) as they arise;
- Whenever overseeing the use of technology in school or settings, such as homework tasks, encourage sensible use, monitor what pupils are doing and consider potential dangers and the age appropriateness of websites;
- Carefully supervise and guide pupils when engaged in learning activities involving online technology (including extra-curricular and extended school activities if relevant), supporting them with search skills, critical thinking (e.g. fake news), age-appropriate materials and signposting, and legal issues such as copyright and data law;
- Ensure that pupils do not bring any portable devices into school for the saving or transferring of work (e.g. USB stick, external hard drive etc.)
- Prepare and check all online sources and resources before using within the classroom;
- Encourage pupils to follow their Acceptable Use of Technology Policy, remind them about it and enforce school sanctions;
- Notify the DSL/Online Safety Leads of new trends and issues before they become a problem;

- Take a zero-tolerance approach to cyberbullying including low-level sexual harassment;
- Be aware that you are often most likely to see or overhear online safety issues (particularly relating to bullying and sexual harassment and violence) in the playground, corridors, toilets and other communal areas outside the classroom – make sure you inform the DSL/Online Safety Leads following school procedures;
- Receive regular updates from the DSL/Online Safety Leads and have a healthy curiosity for online safety issues;
- Model safe, responsible and professional behaviours in your own use of technology (to include NO use of portable devices for saving/transferring of work such as a USB device, memory stick, external hard drive). This includes outside the school hours and site, and on social media, in all aspects upholding the reputation of the school and the professional reputation of all staff.

3.7 Volunteers, visitors and contractors

Key responsibilities:

- All volunteers/visitors read, understand, sign and adhere to the Volunteer & Visitors Acceptable Use Policy;
- Visitors and contractors listen to a verbal guidance to acceptable use of mobile phones and are monitored by a member of staff should they need to use their mobile devices;
- Volunteers, visitors and contractors must not bring any portable devices into school for the saving or transferring of work (e.g. USB stick, external hard drive etc.)
- Report any concerns, no matter how small, to the Designated Safeguarding Lead/Deputy DSLs/Online Safety Leads;
- Maintain an awareness of current online safety issues and guidance;
- Model safe, responsible and professional behaviours in their own use of technology.

3.8 Pupils

Key responsibilities:

- Read, understand, sign and adhere to their Acceptable Use of Technology Policy at the beginning of each academic year or whenever a new child joins the school;
- Know the implications of misusing the internet and posting inappropriate materials to websites, as this may have legal implications;
- Understand the importance of reporting abuse, misuse or access to inappropriate materials;
- Understand the importance of adopting safe and responsible behaviours and good online safety practice when using digital technologies outside of school;
- I will not bring any portable devices into school for the saving or transferring of work (e.g. USB stick, external hard drive etc.)

- Understand that the school also has the right to take action against them if they are involved in incidents of inappropriate behaviour that involve the pupils' membership of the school community (e.g. cyberbullying, use of images or personal information, sexting);
- Know and understand policies on the use of mobile devices;
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- Understand the benefits/opportunities and risks/dangers of the online world and know who to talk to at school or outside school if there are any problems or concerns.

3.9 Parents

Parents play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. The school takes every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, the school website and information about national and local online safety campaigns.

Key responsibilities:

- Read, sign and promote the school's Parent/Carer Acceptable Use of Technology Policy and read their child's Acceptable Use of Technology Policy and encourage them to follow it;
- Ensure their children do not take any portable devices into school for the saving or transferring of work (e.g. USB stick, external hard drive etc.)
- Consult with the school if they have any concerns about their children's and others' use of technology;
- Set up parental controls on devices;
- Ensure their children do not have access to age-inappropriate apps and games (paying attention to the age limits for social media sites such as Facebook and Whatsapp, as well as the PEGI ratings for games);
- Promote safe search engines such as swiggle.org.uk and kids-search.com;
- Use the school website's 'Online Safety Information' as a resource base;
- Talk with their children about online safety and agree boundaries for their online activity and monitor it;
- Promote the appropriate use of digital images and videos taken at school events;
- Promote positive online safety and model safe, responsible and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, visitors, governors, pupils or other parents/carers;
- Be responsible for reporting any concerns to the relevant bodies: app/website/game admin, CEOPs, NSPCC, Childline, Online Safety Leads etc.

4. Education and curriculum

4.1 Educating pupils about online safety

Pupils will be taught about online safety as part of the school's Life Skills curriculum.

In the Early Years Foundation Stage (Reception), pupils will be taught to:

- Foster their understanding of our culturally, socially, technologically and ecologically diverse world.

In Key Stage 1, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

In Key Stage 2, pupils will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

The safe use of social media and the internet will also be covered in other subjects where relevant. The following subjects have the clearest links to online safety:

- PSHE/RSHE – referred to as Life Skills
- Computing
- Citizenship

However, it is the role of all staff to identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum, supporting subject leaders, and making the most of unexpected learning opportunities as they arise.

The school will also use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

4.2. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications sent home, and in information via our website. Online Safety will also be covered during parents' evenings, where appropriate.

This policy will also be shared with parents. If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Headteacher/DSL.

5. Acceptable use of the internet in school

All pupils, parents, staff, volunteers, visitors and governors are expected to sign a policy regarding the acceptable use of the school's ICT systems and the internet. Visitors will be expected to read and agree to the school's terms on acceptable use, if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, visitors and governors (where relevant) to ensure they comply with the above.

More information is set out in the Acceptable Use of Technology Policies in the Appendices.

5.1 Acceptable use by staff

All staff should receive a copy of the Staff Acceptable Use of Technology Policy (see Appendices), which they need to sign and return to the Headteacher for filing in their personnel file.

The Staff Acceptable Use of Technology Policy will be displayed in the staff room as a reminder to staff that they need to safeguard themselves when online.

Staff members have access to the network so that they can obtain age-appropriate resources for their classes and create folders for saving and managing resources. They also have access to Class Dojo so that they can send message to parents of children in their classes, as well as upload photographs and videos linked to their class and the children's learning. Staff should ensure any messages sent via Class Dojo are professional and appropriate.

Staff must not download software onto school computers without reference to the Headteacher or IT Technician.

Staff have a password to access a filtered internet service. This password should **not** be disclosed to anyone and computers and other devices should **not** be left unattended whilst staff are logged in. It is important that staff do not allow pupils to use a computer using an adult's login details as this could expose them to unsuitable materials.

Social networking outside of work hours, on non-school issue equipment, is the personal choice of all school staff. Owing to the public nature of such websites, it is advisable for staff to consider the possible implications of participation.

The following advice should be considered if involved in social networking:

- Staff must **never** add pupils as 'friends' into their personal accounts (including past pupils under the age of 16);
- Staff are strongly advised not to add parents as 'friends' into their personal accounts;
- Staff must **not** post comments about the school, pupils, parents or colleagues including members of the governing board;
- Staff must **not** use social networking sites within lesson times (for personal use);

- Staff should only use social networking in a way that does not conflict with the current National Teachers' Standards;
- Staff should review and adjust their privacy settings to give them the appropriate level of privacy and confidentiality;
- Staff should read and comply with 'Guidance for Safer Working Practice for Adults who Work with Children and Young People' (2015).

5.2 In the event of inappropriate use by staff

If a member of staff is believed to have misused the internet or school messaging services in an abusive or illegal manner, a report must be made to the Headteacher/DSL immediately and then the **Managing Allegations Procedure** and the Safeguarding and Child Protection Policy must be followed to deal with any misconduct and all appropriate authorities contacted. Inappropriate use may lead to disciplinary action.

In the event of accidental misuse, staff must report it to the Headteacher immediately.

5.3. Acceptable use by pupils

All pupils should receive a copy of the appropriate Acceptable Use of Technology Policy for their year group (see Appendices) at the start of each academic year or when joining the school, which needs to be returned to the school office for filing in their blue pupil file. The school will encourage parents/carers to support the policy with their child. This can be shown by signing the Acceptable Use of Technology Policy together so that it is clear to the school that the policy is accepted by the child, with the support of the parent/carer.

These Acceptable Use of Technology Policies detail how children are expected to use the internet and other technologies within school, including the downloading or printing of any materials. The policies are there for pupils to understand what is expected of their behaviour and attitude when using the internet. This will enable them to take responsibility for their own actions. For example, knowing what is polite to write in an email to another child, or understanding what action to take should there be the rare occurrence of sighting unsuitable material. This also includes the deliberate searching for unsuitable materials and the consequences of doing so.

The downloading of materials, for example, music files and photographs, needs to be appropriate and 'fit for purpose' based on research for work and be copyright-free.

File-sharing via email, weblogs or any other means online should be appropriate and be copyright-free when used beyond school.

This policy also applies to the use of social networking sites. Such sites should not be used/accessed in school unless under the direction of a teacher and for a purpose clearly apparent from the learning objective. If social media sites are used, the staff should carry out a risk assessment to determine which tools are appropriate. Social media sites to be used in school include Primary Blogger and Twitter. Parents will give permission for children to access these sites in school as well as permission for images of their child/child's work to be included on the site. In terms of private use of social networking sites by a child, it is generally understood that **children under the age of 13 are not permitted to be registered**, **for instance, on Facebook or Instagram.**

5.4. In the event of inappropriate use by pupils

Should a pupil be found to misuse the online facilities, the following consequences may occur:

- Any pupil found to be misusing the internet by not following the Acceptable Use of Technology Policy may have a letter sent home to their parents/carers explaining the reason for suspending the child's use for a particular lesson or activity;
- Further misuse of the internet may result in the pupil not being allowed to access the internet for a period of time and another letter will be sent home to parents/carers;
- A letter may be sent to parents/carers outlining the breach of the school's Safeguarding and Child Protection Policy where a pupil is deemed to have misused technology against another child or adult;
- In accordance with the Defamation Act (2013), action may be taken against the individual if they have made a defamatory statement about the school or members of staff or governors online, including on social media websites;
- In the event of illegal activities, the school has the duty to involve the police.

5.5. Acceptable use by parents/carers

With all pupils and parents/carers receiving and signing the Acceptable Use of Technology Policies (see Appendices), it is clear to the school that the policies are accepted by the child and the parent/carer. These are also intended to provide support and information to parents/carers when children are using the internet outside school.

Parents and carers will be made aware of their responsibilities regarding their use of social networking. Methods of school communication include the website, newsletters, letters, verbal discussion, text messaging, Tapestry, Class Dojo and Twitter. School policies and documents provide further information regarding appropriate channels of communication and means of resolving differences of opinion. Effective communication following principles of mutual respect is the best means of ensuring the best learning experiences for the child.

Parents/carers should use Class Dojo to communicate about their child's learning and ask any relevant question to the teachers (**between the hours of 8am and 5pm on weekdays only**). **Staff will not reply to messages outside of these times.**

Parents/carers must not post pictures of pupils, other than their own children on networking sites where these photographs have been taken at a school event.

Parents/carers should make complaints through official school channels using the Complaints Policy and Procedure rather than posting them on social networking sites.

Parents/carers must not post or share private conversations between themselves and a member of school staff (e.g. one that has taken place on Class Dojo or Tapestry).

Parents/carers should not post malicious or fictitious comments on social networking sites about any member of the school community.

5.6. In the event of inappropriate use by parents

In the case of inappropriate use of social networking by parents/carers:

- The Governing Board will contact the parent asking them to remove the comments/photographs/images/videos and seek redress through the appropriate channels such as the Complaints Policy and Procedure;
- The Governing Board understands that "There are circumstances in which police involvement is appropriate. These include where postings have a racist element or where violence is threatened or encouraged." Furthermore, "Laws of defamation and privacy still apply to the web and it is unlawful for statements to be written which:
    - expose an individual to hatred, ridicule or contempt;
    - cause an individual to be shunned or avoided;
    - lower an individual's standing in the estimation of right-thinking members of society;
    - disparage an individual in their business, trade, office or profession.

In the event that a member of staff finds themselves, or another adult, on an external website, such as 'Rate My Teacher' or Facebook, as a victim, staff are encouraged to report the incident to the Headteacher, as a matter of urgency.

6. Device usage

6.1. Usage of personal devices including wearable technology

Please read the following in conjunction with Acceptable Use of Technology Policies.

6.1.1. Personal devices

- **All staff who work directly with children** should leave their mobile phones on silent and only use them in private staff areas during school hours. Child/staff data should never be downloaded onto a private phone. If a staff member is expecting an important personal call when teaching or otherwise on duty, they may leave their phone with the school office to answer on their behalf or ask for the message to be left with the school office. They must not use personal numbers to contact pupils under any circumstances. Staff must ensure that there is no inappropriate or illegal content stored on the device and should be aware that using features such as video or sound recording may be subject to the same procedures as taking images from digital or video cameras. Under no circumstances should personal mobile devices be used to take photographs, e.g. on educational visits. The school does not accept responsibility for any theft, loss or damage of any personal mobile device.

  Smart watches/wearable technology can be worn by staff but they must not be used to make calls or take photos during school hours.

- Pupils in Year 5/6 are allowed to bring mobile phones to school as many children walk to and from school on their own. Children who bring a mobile phone to school must turn it off and hand it in upon arrival at school to their class teacher. Phones will be stored securely during the day. However, the school does not accept responsibility for any theft, loss or damage. Important messages and phone calls to or from parents can be made at the school office, who will also pass on messages from parents to pupils in emergencies.

Smart watches/wearable technology must not be worn by pupils.

- Volunteers, visitors, contractors and governors should leave their mobile phones in their pockets and turned off. They will be asked to do this upon arrival at the school, by office staff. Under no circumstances should mobile phones be used in the presence of children or to take photographs or videos. If this is required (e.g. for contractors to take photos of equipment or buildings), permission of the Headteacher should be sought (the Headteacher may choose to delegate this) and photographs should only be taken in the presence of a member of staff.

- Parents are asked to leave their mobile phones in their pockets and turned off when they are onsite. They should ask permission before taking any photos, e.g. of displays in corridors or classrooms, and avoid capturing other children. When at school events, please refer to the Permission for Photographs Form. Parents are asked not to call pupils on their mobile phones during the school day; urgent messages can be passed via the school office.

- Staff, pupils, volunteers, visitors, contractors and parents are not permitted to bring any portable devices onto the school site for the saving or transferring of work (e.g. USB stick, external hard drive etc.)

6.1.2. School devices

Where the school has provided a mobile device to a member of staff, such as a laptop, PDA or mobile phone, only this equipment should be used to conduct school business outside of the school environment.

Exceptions to this are where users access personal information in school in their own time. This activity must not be of a commercial or profit-making nature and must not conflict with school activities.

Printing of private items is not permitted. Under no circumstances must efforts be made to access material normally blocked by the school filtering system.

7. School website

The school website is a key public-facing information portal for the school community (both existing and prospective stakeholders) with a key reputational value. The site is managed by the Headteacher and Administration & Facilities Manager and hosted by Primary Site. The DfE has determined the information which must be available on a school website.

School has the same duty as any person or organisation to respect and uphold copyright law. Sources must always be credited and material only used with permission.

Where pupil work, images or videos are published on the website, their identities will be protected and full names will not be published.

8. Online safety resources

To support online safety at Blundeston CEVC Primary School, we use the following resources:

- Anti-virus and anti-spyware software (Trend Micro 0- supplied by RM)
- Internet filters are supplied and maintained by Suffolk County Council (Smoothwall)
- Accredited Internet Service Provider (ISP) - Smoothwall
- Wireless technology which has been appropriately security enabled
- Firewall maintained by Suffolk County Council
- ICT equipment which is security marked. Any item not issued to named staff needs to be signed out before taking offsite.

9. Monitoring and review

This policy will be monitored and reviewed every three years by the Governing Board, or sooner if new guidance or advice becomes available, either from the Local Authority or DfE.

APPENDICES

A. Staff Acceptable Use of Technology Policy

B. Staff Acceptable Use of Technology Letter

C. Pupil Acceptable Use of Technology Policy (EYFS/KS1)

D. Pupil Acceptable Use of Technology Policy (KS2)

E. Pupil Acceptable Use of Technology Letter

F. Parent/Carer Acceptable Use of Technology Policy

G. Parent/Carer Acceptable Use of Technology Letter

H. Volunteer & Visitor Acceptable Use of Technology Policy

I. Volunteer & Visitor Acceptable Use of Technology Letter

J. Permission for Photographs Form

A

Staff Acceptable Use of Technology Policy

In my role to keep children safe:

I know who the Senior Designated Lead, Deputy DSLs and the Online Safety Leads are.

I will ensure that online safety issues are embedded in all aspects of the curriculum and other activities.

I will help pupils to understand and follow the Online Safety and Acceptable Use of Technology Policies.

I will teach pupils to have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

I will monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices.

I will ensure that pupils do not bring any portable devices into school for the saving or transferring of work (e.g. USB stick, external hard drive etc.)

I understand that pupils should be guided to sites checked as suitable for their use.

I will teach my pupils about safe searches such as swiggle.org.uk and kids-search.com.

I will encourage my pupils to consider the implications of misusing the internet and posting inappropriate materials to websites, as this may result in a temporary ban as a consequence (along with contacting parents) and/or legal implications.

I will keep up-to-date with online safety knowledge that is appropriate for the age group and reinforce it through the curriculum.

How I will keep myself safe when accessing school devices and networks:

Where the school has provided me with a mobile device, such as a laptop, PDA or mobile phone, this equipment should only be used to conduct school business outside of the school environment.

I will not bring any portable devices into school for the saving or transferring of work (e.g. USB stick, external hard drive etc.)

I will only use the school's technology resources and systems for purposes deemed 'reasonable' by the Headteacher and Governing Board.

I will not reveal my password(s) to anyone.

If my password is compromised, I will make sure I change it immediately.

I will not use anyone else's passwords, and if they reveal it to me, then I will advise them to change it.

I understand that any workplace devices should have PIN/password protection and that they should not be left unattended with an app/website logged on/open/active.

I will not allow pupils to use a computer using an adult's login details as this could expose them to unsuitable material.

I will not allow unauthorised individuals to access my emails, intranet, network etc.

I am aware that I am not permitted to print private items in the workplace.

I am aware that under no circumstances must efforts be made to access materials normally blocked by the school filtering system.

I will not use technology in school to view material that is illegal, inappropriate or likely to be deemed offensive. This includes, but is not limited to, sending obscene emails, gambling and viewing pornography or other inappropriate content.

How I will keep safe when using multimedia:

I understand that any photographs or video clips uploaded should not have a file name of a child, especially where these may be uploaded to a school website.

I understand that group photographs are preferable to photographs of individual children and should not include children in compromising positions or in inappropriate clothing.

The class teachers will be responsible for, and will need to decide, how photographs will be used, including where they will be stored securely.

All photographs will be deleted after a term.

I know that photographs should only ever include the child's first name.

I know that it is current practice by external media such as local and national newspapers to include the full name of pupils in their publications. Photographs of pupils should only be used after permission has been given by a parent/carer for external use.

I am aware that, under no circumstances, should any multimedia (photos, videos) be kept on a personal device.

How I will keep myself safe when communicating:

I understand that when accessing Class Dojo, Twitter, Tapestry, school email or the school website from home, the same Acceptable Use Policy will apply.

It is imperative that the device has PIN/password protection and that they are not left unattended with an app/website logged on/open/active.

I am expected to monitor the use of emails and Class Dojo communications between home and school, between the working hours of 8am and 5pm on weekdays.

I know that I should use my school-provided email address, Tapestry or Class Dojo for any communication between home and school.

I will never share my personal details with pupils/parents such as private email address, telephone number, home address or social media/networking names.

I will ensure my profile name does not identify me, in case pupils or parents try and search for me.

If a pupil or parent attempts to contact me via a social media site, I will decline this request immediately and inform the Headteacher that the request has been made. I will then review my privacy and security settings to ensure the situation does not happen again.

I will use good 'housekeeping' and delete read emails regularly.

I will always communicate online in a polite and respectful manner.

How I will keep myself safe with my personal devices:

I am aware that I am allowed to bring in personal mobile phones or devices for my own use (not within lesson/contact time).

I am aware that I am not allowed to bring any portable devices into school for the saving or transferring of work (e.g. USB stick, external hard drive etc.)

I am aware that I must not use personal numbers/emails/social media sites to contact school pupils/parents under any circumstances (use the 'caller withheld' function if out on a school trip and off premises).

I will regularly review my privacy and security settings on my social media accounts to ensure they still offer the level of security needed.

All personal devices must be kept out of sight and turned off or on silent during teaching hours.

I will not have any inappropriate or illegal content stored on the device.

I will not take any pictures/videos of pupils on my personal devices and I won't add any pictures/videos on to any personal social media sites unless it is a 'school account'.

Under no circumstances should personal mobile devices be used to take photographs/videos, e.g. on educational visits.

The school is not responsible for any theft, loss or damage of any personal mobile device.

Smart watches/wearable technology can be worn by staff but they must not be used to make calls or take photos during school hours.

How I will keep myself safe with my social media platforms/networking:

I will consider the risks and consequences of anything that I post to any web or social networking site, as inappropriate comments or images can reflect poorly on an individual and can affect future careers.

In the event that a member of staff finds themselves or another adult on an external website, such as 'Rate My Teacher', or Facebook, as a victim, staff are encouraged to report incidents to the Headteacher, as a matter of urgency.

I am aware that I can access and use social networking outside of work hours, on non-school issue equipment (this is my own personal choice).

Owing to the public nature of such websites, it is advisable for staff to consider the possible implications of participation. The following advice should be considered if involved in social networking:

 Staff must **never** add pupils as 'friends' into their personal accounts (including past pupils under the age of 16).

 Staff are **strongly advised** not to add parents as 'friends' into their personal accounts.

 Staff **must not** post comments (information or opinions) about the school, pupils, parents or colleagues, including members of the Governing Board.

 Staff **must not** use social networking sites within lesson times (for personal use).

 Staff should only use social networking in a way that does not conflict with the current Teachers' Standards.

 Staff should review and adjust their privacy and security settings to give them the appropriate level of privacy and confidentiality.

 Staff should read and comply with 'Guidance for Safer Working Practice for Adults who Work with Children and Young People' (2015).

 Inappropriate use by staff should be referred to the Headteacher in the first instance and may lead to disciplinary action. If there are concerns about the Headteacher's conduct, these should be raised with the Chair of Governors.

 If I am on a social media site with parents from the school, I **must not** comment on any posts, even if I want to defend the school, its reputation or a member of the school community. I will report any incidents of slander or inappropriate references to the school or members of the school community to the Headteacher, as a matter of urgency.

How I will keep myself safe with my data and GDPR:

I will make sure that all documents and data are saved, accessed and deleted in accordance with GDPR regulations.

I will follow the correct procedures for any data required to be taken from the school. Secure, One drive is ONLY to be used for the saving and storing of data along with any school devices (Teacher laptops, staff ipads etc)

I will report any suspected misuse or problem to the Headteacher for investigation/action/sanction.

I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the Headteacher.

I understand that I am responsible for reporting issues:

I know how to deal with any unsuitable material that is found in internet searches (e.g. screen shot, copy and paste into a word document with date/time and search words and pass on to the Online Safety Leads and/or Headteacher).

I know how to deal with any issue around online safety, online safety, cyberbullying, inappropriate use of games/apps and know how to use the CPOMS system.

I understand that I have to report incidents of personally directed "bullying" or other inappropriate behaviour via the internet or other technologies to the Headteacher.

I understand that I have to report incidents of staff, pupils and visitors using external devices (such as USB sticks and external hard drives) to the Headteacher.

If a member of staff, volunteer/visitor is believed to have misused the internet or school messaging services in an abusive or illegal manner, a report must be made to the Headteacher immediately and then the Managing Allegations Procedure and the Safeguarding and Child Protection Policy must be followed to deal with any misconduct and all appropriate authorities contacted.

I am aware that in the event of an allegation being made against the Headteacher, the Chair of Governors must be informed immediately.

In the event of accidental misuse, I know that I must report it to the Headteacher immediately.

I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour.

I understand that, in accordance with the Defamation Act (2013), action may be taken against me if I make defamatory statements about the school or members of staff online, including on social media websites.

I understand that in the event of illegal activities, the school has the duty to involve the police.

I understand that the school’s Online safety Policy covers my actions out of school, as well as in school.

First name:	**Surname:**
Signed:	**Dated:**

I am signing to say that I have read and understood the Staff Acceptable Use of Technology Policy and that I agree to follow it. I understand that there may be consequences for my own actions when online if I breach this policy.

B

Staff Acceptable Use of Technology Letter

Dear

At Blundeston CEVC Primary School, we recognise that staff can be vulnerable to online risks. Social media can blur the definitions of personal and working lives; it is important that all members of staff at the school take precautions to protect themselves both professionally and personally online.

To this end, we request that all members of staff sign the attached Acceptable Use of Technology Policy.

Additional advice and guidance for professionals is available locally through the Local Authority safeguarding service, or nationally through professional unions and/or the professional online safety helpline (www.saferinternet.org.uk/about/helpline).

Failure to follow this guidance and the school's Staff Code of Conduct could lead to disciplinary action, so it is crucial that all staff understand how to protect themselves online.

Please don't hesitate to speak to me or one of the Online Safety Leads if you have any queries or concerns regarding this.

Best wishes,

Helen Laflin

Helen Laflin
Headteacher

C

Pupil Acceptable Use of Technology Policy (EYFS and KS1)

This is how I stay safe when I use computers:

I will ask an adult before I use a computer/iPad.

I will not bring any devices into school from home (e.g. USB/memory sticks etc.)

I will not wear a smart watch during school hours.

I will 'log off' when I leave a computer/iPad/website.

I will only use activities and websites that an adult has told me I am allowed to use.

I will ask an adult for help if I am not sure what to do or think I have done something wrong.

I will tell an adult if something upsets me that I see on the screen.

I will tell an adult if someone I don't know contacts me.

I will take care of the computers, iPads and other equipment in school.

I know that if I break the rules then I may not be allowed to use the computers/internet.

I know that if I break the rules then my parents may be contacted.

Child:

First name:	**Surname:**
Date:	

D

Pupil Acceptable Use of Technology Policy (KS2)

This is how I stay safe when I use computers, to ensure my own safety and show respect towards others:

I will ask an adult before I use a computer/iPad.

I will not bring any portable devices into school for the saving or transferring of work (e.g. USB stick, external hard drive etc.)

I will only use suggested activities and websites that an adult has told me that I am allowed to use.

I know how to "safe search" and can use the internet in a sensible manner (avoiding plagiarism, upholding copyright regulations and using appropriate forms of communication).

I will keep any passwords private and not try to use any other person's username and/or password.

I will not share personal information about myself or others when online.

I am aware that when communicating online, I must not arrange to meet up with anyone unfamiliar, in order to keep myself safe. If someone online suggests I meet them, I will tell a trusted adult immediately.

I will communicate with others online in a polite and sensible manner.

I will ask an adult for help if I am not sure what to do or think I have done something wrong.

I will tell an adult immediately if I see anything inappropriate or if someone I don't know contacts me.

I will not upload or add any images, videos, sounds or text that could upset any member of the school community.

I understand the importance of reporting abuse, misuse or access to inappropriate materials and I know how to do this (I can talk to my teacher, the Digital Leaders, Head Teacher or the Online Safety Leads).

I will take care of the computers, iPads and other equipment in school.

Year 5/6 ONLY:

I know that I am allowed to bring my mobile phone into school if I walk to or from school. I understand it will be kept securely for the duration of the school day (not to be accessed and/or used). I will turn my phone off before entering the school site and handing it in and will not turn it on again until I leave the school site.

I will not wear a smart watch during school hours.

I understand that the school accepts no responsibility for any theft, loss of damage to mobile phones whilst they are in school.

I understand that I am responsible for my actions, both in and out of school:

I understand that the school has the right to take action against me if I am involved in incidents of inappropriate behaviour online.

I know that if I break the rules (misusing the internet, posting inappropriate materials etc.) then I may not be allowed to use the computers/internet in school and I may be reported to the police.

If I break the rules, then my parents may be contacted.

I understand that, in accordance with the Defamation Act (2013), action may be taken against me if I make defamatory statements about the school or members of staff online, including on social media websites.

I understand that in the event of illegal activities, the school has the duty to involve the police.

I understand that the school's Online safety Policy covers my actions out of school as well as in school.

Child:

First name:	**Surname:**
Date:	

E

Pupil Acceptable Use of Technology Letter

Dear

All children at our school use computer facilities, including internet access, as an essential part of learning. You will have the opportunity to access a wide range of technology resources. This includes access to:

- Computers, laptops, iPads and other digital devices
- The internet, which may include search engines and educational sites
- Class Dojo
- Digital cameras, webcams and video cameras
- Interactive boards/screens

At Blundeston Primary School, we recognise the essential and important contribution that technology plays in promoting your learning and development, both at school and at home. However, we also recognise there are potential risks. The school will take all reasonable precautions to ensure that you are as safe as possible when using school equipment and will work together with you and your family to help you stay safe online. We want to ensure that all members of our community are safe and responsible users of technology.

We will support you to:

- ✓ Become empowered and responsible digital creators and users
- ✓ Use our resources and technology safely, carefully and responsibly
- ✓ Be kind online and help us to create a community that is respectful and caring, on and offline
- ✓ Be safe and sensible online, and always know that you can talk to a trusted adult if you need help

Should you have any worries about online safety then you can speak with one of our Digital Leaders, Miss Laflin or one of the Online Safety Leads (Miss Gowen and Miss Clarke).

You can also access support through the school and via other websites such as www.thinkuknow.co.uk and www.childline.org.uk.

We would like you and your family to read our school's Acceptable Use Policy and return the attached slip.

We look forward to helping you become a positive and responsible digital citizen.

H.Laflin

Miss H. Laflin
Headteacher

F

Parent/Carer Acceptable Use of Technology Policy

How I will support my child in staying safe online:

I will discuss the Acceptable Use of Technology Policy with my child and ensure it is followed.

I will ensure my child does not take any portable devices into school for the saving or transferring of work (e.g. USB stick, external hard drive etc.)

I will set up parental controls on devices at my discretion and where I see fit.

I will promote safe search engines such as swiggle.org.uk and kids-search.com.

I will help my child in downloading/using/playing age-appropriate apps/websites/games.

I will regularly monitor my child's online activity.

I will talk regularly to my child about online activity and safety.

I will use the school website's 'Online Safety Information' zone as a resource base.

I will have a 'home/family agreement' on boundaries for safe online activity.

I will support my child to report any concerns with the relevant bodies: App/website/game admin, CEOPs, NSPCC, Childline, school Online Safety Leads (Miss Clarke and Miss Gowen).

How the school will keep my child safe online:

The school will deliver online safety education to my child.

They will teach my child to use the internet in a safe and responsible manner through all curriculum subjects.

My child will be taught to tell an adult immediately about any inappropriate materials or contact from someone they do not know.

The school will teach the importance of reporting abuse, misuse or access to inappropriate materials and how to do so.

My child will be taught research skills and the need to avoid plagiarism and uphold copyright regulations.

The school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems.

The school will ensure that pupils do not bring any portable devices into school for the saving or transferring of work (e.g. USB stick, external hard drive etc.)

The school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and by using mobile technologies.

I understand that my child's activity on the school's ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of this Acceptable Use Policy.

Staff will check all online material used in lessons before sharing with the children for appropriateness and in line with the latest Terms of Service (July 2019) will only show YouTube clips to those children who have parental permission.

How I will keep myself safe when online:

When communicating online, I will do so in a polite and sensible manner.

I can use Class Dojo to communicate with my child's class teacher and ask any relevant questions (between the hours of 8am and 5pm on weekdays).

I am aware that it is not advised to have school staff as 'friends' on my personal social media accounts.

I am aware of privacy settings and will set them to the appropriate level.

I know that I must not post pictures/videos of pupils, other than my own child, on social media sites where the photographs have been taken at a school event.

I know that I must make complaints through official school channels and in accordance with the school's Complaints Policy, rather than posting them on social media sites.

I understand that I should not post unkind, malicious, fictitious, libellous or defamatory comments on social media sites about the school or any member of the school community. This includes campaigns against the school or any member of the school community.

I understand that I am responsible for my actions, both in and out of school:

I am aware that the school will contact me (by phone call, meeting or letter) if I have breached the Acceptable Use Policy, to explain my actions and their implications.

I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour.

I understand that, in accordance with the Defamation Act (2013), action may be taken against me if I make defamatory statements about the school or members of staff online, including on social media websites.

I understand that in the event of illegal activities, the school has the duty to involve the police.

As a school, we understand that "There are circumstances in which police involvement is appropriate. These include where postings have a racist element or where violence is threatened or encouraged." Furthermore, "Laws of defamation and privacy still apply to the web and it is unlawful for statements to be written which

□ expose an individual to hatred, ridicule or contempt

□ cause an individual to be shunned or avoided

□ lower an individual's standing in the estimation of right-thinking members of society or

□ disparage an individual in their business, trade, office or profession."

I give permission for staff to share online age-appropriate educational material with my child, including clips from YouTube.

PLEASE CONTACT THE SCHOOL TO OPT-OUT OR DISCUSS THIS AGREEMENT.

G

Parent/Carer Acceptable Use of Technology Letter

Dear Parent/Carer,

All pupils at Blundeston CEVC Primary School use computer facilities and have internet access, as an essential part of learning as required by the National Curriculum. Your child will have the opportunity to access a wide range of information and communication technology (ICT) resources. This includes access to:

- Computers, laptops, iPads and other digital devices
- The internet, which may include search engines and educational sites
- Digital cameras, webcams and video cameras
- Interactive boards/screens

The school recognises the essential and important contribution that technology plays in promoting children's learning and development, believing it offers a fantastic range of positive activities and experiences. We do recognise, however, that this can also bring risks. We take your child's online safety seriously and, as such, will take all reasonable precautions, including monitoring and filtering systems, to ensure that our pupils are safe when they use our internet and systems. We recognise though that no technical system can replace online safety education and believe that children themselves have an important role to play in developing responsible behaviour.

To support the school in developing your child's knowledge and understanding about online safety, we request that you read the attached pupil and parent/carer Acceptable Use of Technology Policy, discuss the content of them with your child (as you see appropriate) and return the attached signature slips.

Early Years/KS1

We understand that your child is too young to give informed consent on his/her own; however, we feel it is good practice to involve them as much as possible in the decision-making process, and believe a shared commitment is the most successful way to achieve this. Hopefully, you will also find this Acceptable Use Policy provides you with an opportunity for conversations between you and your child about safe and appropriate use of technology, both at school and at home.

We request that all parents support our approach to online safety by role modelling safe and positive online behaviour and by discussing online safety whenever children access technology at home. Parents can visit the school website for more information about our approach to online safety.

Parents/carers may also like to visit the following links for more information about keeping children safe online:

- www.thinkuknow.co.uk
- www.childnet.com
- www.nspcc.org.uk/onlinesafety
- www.saferinternet.org.uk
- www.internetmatters.org

Should you wish to discuss the matter further, please do not hesitate to contact the school's Online Safety Leads.

Best wishes,

H.Laflin

Miss Helen Laflin
Headteacher

H

Volunteer & Visitor Acceptable Use of Technology Policy

In my role to keep children safe:

I know who the Senior Designated Lead, Deputy DSLs and the Online Safety Leads are.

I will help pupils to understand and follow the Online Safety and Acceptable Use of Technology Policies.

Where appropriate, I will monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices.

I will ensure that pupils do not bring any portable devices in to school for the saving or transferring of work (e.g. USB stick, external hard drive etc.) and I will inform a member of staff immediately.

I understand that pupils should be guided to sites checked as suitable for their use.

How I will keep myself safe when accessing school devices and networks:

I will only use the school's technology resources and systems for purposes deemed 'reasonable' by the Headteacher and Governing Board.

I will not bring any portable devices into school for the saving or transferring of work (e.g. USB stick, external hard drive etc.)

I will not use anyone else's passwords, and if they reveal it to me, then I will advise them to change it.

I understand that any workplace devices should have PIN/password protection and that they should not be left unattended with an app/website logged on/open/active.

I will not allow pupils to use a computer using an adult's login details as this could expose them to unsuitable material.

I will not allow unauthorised individuals to access my emails, intranet, network etc.

I am aware that I am not permitted to print private items in the workplace.

I am aware that under no circumstances must efforts be made to access materials normally blocked by the school filtering system.

I will not use technology in school to view material that is illegal, inappropriate or likely to be deemed offensive. This includes, but is not limited to, sending obscene emails, gambling and viewing pornography or other inappropriate content.

How I will keep safe when using multimedia:

I understand that any photographs or video clips uploaded should not have a file name of a child, especially where these may be uploaded to a school website.

I understand that group photographs are preferable to photographs of individual children and should not include children in compromising positions or in inappropriate clothing.

The class teachers will be responsible for, and will need to decide, how photographs will be used, including where they will be stored. All photographs will be deleted after a term.

I know that photographs should only ever include the child's first name.

I know that it is current practice by external media such as local and national newspapers to include the full name of pupils in their publications. Photographs of pupils should only be used after permission has been given by a parent/carer for external use.

I am aware that, under no circumstances, should any multimedia (photos, videos) be kept on a personal device.

How I will keep myself safe when communicating:

I will never share my personal details with pupils/parents such as private email address, telephone number, home address or social media/networking names.

I will ensure my profile name does not identify me in case pupils or parents try and search for me.

If a pupil or parent attempts to contact me via a social media site, I will decline this request immediately and inform the Headteacher that the request has been made. I will then review my privacy and security settings to ensure the situation does not happen again.

I will always communicate online in a polite and respectful manner.

How I will keep myself safe with my personal devices:

I am aware that I am allowed to bring in personal mobile phones or devices for my own use (not within lesson times).

I am aware that I am not allowed to bring any portable devices into school for the saving or transferring of work (e.g. USB stick, external hard drive etc.)

I must not use personal numbers/emails/social media sites to contact school pupils/parents under any circumstances.

I will regularly review my privacy and security settings on my social media accounts to ensure they still offer the level of security needed.

All personal devices must be kept out of sight and turned off or on silent during teaching hours.

I will not have any inappropriate or illegal content stored on the device.

I will not take any pictures/videos of pupils on my personal devices and I won't add any pictures/videos on to any personal social media sites unless it is a 'school account'.

Under no circumstances should personal mobile devices be used to take photographs/videos, e.g. on educational visits.

The school is not responsible for any theft, loss or damage of any personal mobile device.

Smart watches/wearable technology can be worn by volunteers/visitors but they must not be used to make calls or take photos during school hours.

How I will keep myself safe with my social media platforms/networking:

I will consider the risks and consequences of anything that I post to any web or social networking site, as inappropriate comments or images can reflect poorly on an individual and can affect future careers.

In the event that a volunteer/visitor finds themselves or another adult on an external website, such as Facebook, as a victim, they are encouraged to report incidents to the Headteacher, as a matter of urgency.

I am aware that I can access and use social networking outside of school, on non-school issue equipment (this is my own personal choice).

Owing to the public nature of such websites, it is advisable for volunteers/visitors to consider the possible implications of participation. The following advice should be considered if involved in social networking:

 Volunteers/visitors must **never** add pupils as 'friends' into their personal accounts (including past pupils under the age of 16).

 Volunteers/visitors are **strongly advised** not to add parents as 'friends' into their personal accounts.

 Volunteers/visitors **must not** post comments (information or opinions) about the school, pupils, parents or colleagues, including members of the Governing Board.

 Volunteers/visitors **must not** use social networking sites within lesson times (for personal use).

 Volunteers/visitors should review and adjust their privacy and security settings to give them the appropriate level of privacy and confidentiality.

 Inappropriate use by volunteers/visitors should be referred to the Headteacher in the first instance and may lead to disciplinary action. If there are concerns about the Headteacher's conduct, these should be raised with the Chair of Governors.

 If I am on a social media site with parents from the school, I **must not** comment on any posts, even if I want to defend the school, its reputation or a member of the school community. I will report any incidents of slander or inappropriate references to the school or members of the school community to the Headteacher, as a matter of urgency.

How I will keep myself safe with my data and GDPR:

I will make sure that all documents and data are saved, accessed and deleted in accordance with GDPR regulations.

I will report any suspected misuse or problem to the Headteacher for investigation/action/sanction.

I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the Headteacher.

I understand that I am responsible for reporting issues:

I know to speak to the Headteacher/Online Safety Leads about any issue around online safety, cyberbullying, inappropriate use of games/apps etc.

I understand that I have to report incidents of personally directed "bullying" or other inappropriate behaviour via the internet or other technologies to the Headteacher.

I understand that I have to report incidents of staff, pupils and visitors using external devices (such as USB sticks and external hard drives) to the Headteacher.

If a member of staff or volunteer/visitor is believed to have misused the internet or school messaging services in an abusive or illegal manner, a report must be made to the Headteacher immediately and then the relevant procedures must be followed to deal with any misconduct and all appropriate authorities contacted.

I am aware that in the event of an allegation being made against the Headteacher, the Chair of Governors must be informed immediately.

In the event of accidental misuse, I know that I must report to the Headteacher immediately.

I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour.

I understand that, in accordance with the Defamation Act (2013), action may be taken against me if I make defamatory statements about the school or members of the school community online, including on social media websites.

I understand that in the event of illegal activities, the school has the duty to involve the police.

I understand that the school's Online Safety Policy covers my actions out of school, as well as in school.

First name:	**Surname:**
Signed:	**Dated:**

I am signing to say that I have read and understood the Volunteer & Visitor Acceptable Use of Technology Policy and that I agree to follow it. I understand that there may be consequences for my own actions when online if I breach this policy.

Volunteer & Visitor Acceptable Use of Technology Letter

Dear

At Blundeston CEVC Primary School, we recognise that volunteers and visitors can be vulnerable to online risks. Social media can blur the definitions of personal and working lives; it is important that all volunteers and visitors at the school take precautions to protect themselves both professionally and personally online.

To this end, we request that all volunteers and visitors sign the attached Acceptable Use of Technology Policy.

Failure to follow this guidance and the school's Volunteer & Visitor Code of Conduct could lead to disciplinary action, so it is crucial that all volunteers and visitors understand how to protect themselves online.

Please don't hesitate to speak to me or one of the Online Safety Leads if you have any queries or concerns regarding this.

Best wishes,

Helen Laflin

Miss Helen Laflin
Headteacher

J

BLUNDESTON CEVCP SCHOOL – PERMISSION FOR PHOTOGRAPHS

Child's name:……(PLEASE COMPLETE)

Date:……..

Dear Parent/Guardian,

At Blundeston CEVCP School, we sometimes take photographs of pupils. We use these photos on the school's website and on display boards around school. Occasionally they are shared with the local press to advertise activities taking place in the school.

We would like your consent to take photos of your child, and use them in the ways described above. If you're not happy for us to do this, that's no problem – we will accommodate your preferences.

Please tick the relevant box(es) below and return this form to school.

I am happy for the school to take photographs of my child. ☐

I am happy for photos of my child to be used on the school website. ☐

I am happy for photos of my child to be used on Twitter. ☐

I am happy for photos of my child to be used in internal displays. ☐

I am happy for photos of my child to be used in the local paper (i.e. The Journal). ☐

I am **NOT** happy for the school to take or use photos of my child. ☐

If you change your mind at any time, you can let us know by emailing admin@blundeston.suffolk.sch.uk, calling the school on 01502 730488, or just popping in to the school office.

If you have any other questions, please get in touch.

Why are we asking for your consent?

You may be aware that new data protection rules came into force in May 2018. To ensure we are meeting the new requirements, we need to seek your consent to take and use photos of your child. We really value using photos of pupils, to be able to showcase what pupils do in school and show what life at our school is like to others, so we would appreciate you taking the time to give consent.

Parent or carer's signature: _____

Date: _____