Wootton-by-Woodstock CE Primary School

Policy Agreed: February 2019
Person Responsible: Jo Palmer
To be reviewed: February 2022

Policy for E-safety 2019

Definition

All schools have a responsibility under the Children Act 2004 to safeguard and promote the welfare of pupils. An e-safety strategy enables schools to create a safe e-learning environment that:

- promotes the teaching of ICT within the curriculum.
- protects children from harm.
- safeguards staff in their contact with pupils and their own use of the internet.
- ensures the school fulfils its duty of care to pupils.
- provides clear expectations for all on acceptable use of the internet.

Intent

To ensure that all staff, pupils and their parents/carers will:

- behave at all times within the terms of current legislation and the expectations of the school community;
- only use school resources to develop the pupils' skills and knowledge in the context of the wider school curriculum;
- ensure internet use and access is appropriate and controlled;
- prevent misuse of internet connected devices;
- make careful and considerate use of the school's resources, report faults and work in a way that minimises the risk of introducing computer viruses to the system;
- recognise when material is inappropriate and know how to deal with encountering something which causes a feeling of discomfort
- protect everyone in school from harmful or inappropriate material accessible via the internet or transportable on computer media;
- use email and similar systems appropriately;
- recognise the responsibility to maintain the privacy of individuals;
- know and abide by the schools E-Safety Policy.

Wootton-by-Woodstock Primary School expects that all parents and pupils will sign the 'Acceptable Use Agreement' referring to the responsible use of resources and the internet.

This policy relates to all children and adults who use any ICT equipment in school – this may include PCs, laptops, tablets, smart phones, memory sticks or any other new technology with similar applications. It also relates to children and adults working off-site, for example at home, but accessing the school website or other applications recommended by school as part of school work.

Implementation

<u>Responsibility</u>

One of the key features of the school's e-safety strategy is teaching pupils to protect themselves and behave responsibly while on-line. All teaching staff play a role in imparting rules about e-safety.

Wootton-by-Woodstock

ODST Oxford Diocesan Schools Trust

The Curriculum

Teaching and Learning

E-safety is taught and promoted through all curriculum areas. Pupils are taught a planned e-safety curriculum as part of computing/PSHE and other lessons and this is regularly revisited for effectiveness. Pupils are taught

- the benefits and risks of using the internet
- how their behaviour can put themselves and others at risk
- what strategies they can use to keep themselves safe
- what to do if concerned about something they've seen on the internet
- who to contact with concerns
- to be critically aware of the materials and content they access online and be guided to validate the accuracy of information
- to respect copyright when using material accessed on the internet
- to understand the need for the pupil 'Acceptable Use Agreement' and encouraged to adopt safe and responsible use both within and outside school
- that the school has a 'no blame policy' and to report any e-safety incidents
- that the school has a "no tolerance" policy regarding cyber bullying
- that behaviour that breaches acceptable use policies will be subject to sanctions and disciplinary action

Safe Teaching Practice

Staff are aware of the importance of maintaining professional standards of behaviour with regards to their own internet use. Staff must be familiar with the following statements to ensure that their behaviour is not open to misinterpretation and to safeguard them from misplaced or malicious allegations. (See Allegations Policy)

Staff should

- act as good role models in their use of digital technologies, the internet and mobile devices
- be vigilant in monitoring the content of the websites the young people visit.
- guide pupils to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Request that blocked sites are temporarily accessible where pupils research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. Any request to do so, should be auditable, with clear reasons for the need.
- take opportunities to remind pupils of expectations on internet use to keep safe.

- Teachers may use PSHE lessons as a forum for discussing e-safety.
- Photographic and video images of pupils may only taken in connection with educational purposes, e.g. school trips. (See Codes of Conduct)
- Staff may only use and store images on the school computer system or school iPads.
- Staff must be particularly careful regarding any comments communicated over the internet.
- Staff must not engage in any conversation with pupils via instant messaging or social networking sites.
- When making contact with parents or pupils by telephone, staff must only use school equipment. Pupil or parent numbers may not be stored on a staff member's personal mobile phone.
- Staff will ensure that personal data relating to pupils is stored securely if taken away from the school premises.
- Rules regarding safe internet use are displayed in all classrooms.

Safe Use of ICT

Internet and search engines

• When using the internet, children receive the appropriate level of supervision for their age and understanding.
• Children are supervised at all times when using the internet.
• Pupils are not allowed to aimlessly "surf" the internet and all use should have a clearly defined educational purpose.
• Despite filtering systems, it is still possible for pupils to inadvertently access unsuitable websites; to reduce risk, teachers plan use of internet resources ahead of lessons by checking sites.
• Where access to blocked websites is required for educational purposes, this should be agreed with the Headteacher, for temporary access. Teachers must notify the SBM once access is no longer needed to ensure the site is blocked.

Evaluating and using internet content

Teachers must teach pupils efficient research skills and how to critically evaluate information retrieved by:
• questioning the validity of the source of the information
• carrying out comparisons with alternative sources of information
• considering whether the information is current.
Pupils are taught the importance of respecting copyright, correctly quoting sources and told that plagiarism is against the rules of the school.

Emails

Pupils are taught not to disclose personal contact details via email correspondence.
• All email communications must be polite; if a pupil receives an offensive email, they should not reply but tell a teacher immediately.
Pupils are warned that any bullying via email will not be tolerated and will be dealt with in accordance with the school behaviour and anti-bullying policy.
• Users should be aware that use of e-mail is for the purposes of education or school business only, and all emails may be monitored.
• Pupils must not open attachments if they are unsure of the content or have no knowledge of the sender.

Social networking sites and chat rooms

The use of social networking sites (such as Facebook or Twitter) and chat rooms is not permitted at school, and these sites are blocked. Staff must also be aware of maintaining professional codes of conduct in their own personal use of such media and must not network socially with pupils or parents of pupils at the school. (Please see Social Media Policy)

The school website

• Content may not be uploaded onto the school website unless it has been authorised by the headteacher, and is not in breach of copyright.
• The SBM is responsible for uploading materials onto the website.
• To ensure the privacy and security of staff and pupils, the only contact details on the website are the school address, email and telephone number.
• Children's full names must never be published on the website.
• Links to any external websites are regularly reviewed to ensure that their content is appropriate.
Please see ICT Security Policy

Photographic and video images

• Where photographs or videos of children are used, written permission is obtained from parents or carers.
• Children's names are never to be published where their photograph or video is being used.

• Staff will ensure children are suitably dressed to reduce the risk of inappropriate use of images.
• Images will be securely stored only on the school's computer system.
Please see the Codes of Conduct and Social Media policies.

Responding to incidents

• All incidents and complaints relating to e-safety and unacceptable internet use will be reported to the Headteacher. All incidents, whether involving pupils or staff, must be recorded by the Headteacher.
• Where the incident or complaint relates to a member of staff, the matter must always be referred to the Headteacher for action. Incidents involving the Headteacher must be reported to the Chair of Governors.
• The Headteacher will keep a log of all e-safety incidents and complaints and regularly review the information for evidence of emerging patterns of individual behaviour or weaknesses in the school's e-safety system, using these to update the e-safety policy.
• E-safety incidents involving safeguarding issues, for example, contact with inappropriate adults, are reported to the designated lead for child protection, who will make a decision as to whether to refer the matter to the police and/or Safeguarding and Social Care in conjunction with the Headteacher. E-safety strategies and polices are intended to reduce the risk to pupils whilst online, but cannot completely rule out the possibility that pupils may access unsuitable material on the internet. Wootton-by-Woodstock Primary School cannot accept liability for material accessed or any consequences of internet access, but all reasonable precautions will be taken to ensure a safe e-learning environment.

<u>Unintentional access of inappropriate websites</u>
If a pupil or teacher accidently opens a website with distressing or inappropriate content, teachers must immediately close the screen.
• Teachers will reassure pupils that they have done nothing wrong and discuss the incident with the class to reinforce the e-safety message, demonstrating the school's "no blame" approach.
• The incident must be reported to the Headteacher with details of the website address.
• The Headteacher will liaise with the school's ICT technician to ensure that access to the site is blocked and the school's filtering system reviewed to ensure it remains appropriate.

<u>Intentional access of inappropriate websites by a pupil</u>
If a pupil deliberately accesses inappropriate websites, they will be subject to appropriate sanctions.
• The incident will be reported to the Headteacher with details of the website address.
• The Headteacher will liaise with the school's ICT technician to ensure that access to the site is blocked.
• The pupil's parents will be notified of the incident and what action will be taken.

<u>Inappropriate use of the internet by staff</u>

• Staff witnessing misuse of the internet by a colleague, must report this to the Headteacher immediately.
• A note will be recorded on the e-safety incident report form.
• The Headteacher will take necessary disciplinary action and report the matter to the school Governing Body and police where appropriate.

Cyber Bullying

Cyber bullying is defined as the use of the internet to deliberately hurt or upset someone. The internet allows bullying to continue past school hours and invades the victim's home life and personal space. It also allows distribution of hurtful comments and material to a wide audience.
Bullying may take the form of:
• rude, abusive or threatening messages via email or text
• posting insulting, derogatory or defamatory statements on blogs or social networking sites
• setting up websites that specifically target the victim
• making or sharing derogatory or embarrassing videos of someone via mobile phone or email

Cyber bullying can affect both pupils and staff. It could be a criminal offence under the Harassment Act 1997 or the Telecommunications Act 1984.

Dealing with incidents

• Any incidents of cyber bullying must be reported to the Headteacher who will record the incident and ensure that it is dealt with in line with the school's anti-bullying policy.
• Where incidents are extreme or continue over a period of time, they may be reported to the police.
• As part of e-safety awareness and education, pupils will be told of the "no tolerance" policy for cyber bullying and encouraged to report any incidents.
• Pupils are taught to only give out email addresses to people they trust, not to respond to offensive messages, and to report the matter to their parents and teacher immediately.
• Proof of bullying (e.g. texts, emails or comments on websites) will be kept as evidence.

Risk from inappropriate contacts

• All concerns relating to inappropriate contacts will be reported to the child protection designated person immediately.
• The child protection designated person will discuss the matter with the referring teacher and where appropriate, speak to the pupil involved, before deciding whether or not to make a further referral.
• The police will always be contacted if there is a concern that the child is at immediate risk, e.g. if they arrange to meet an adult after school.
• Teachers will advise the pupil how to terminate the contact and change contact details where necessary to ensure no further contact.
• The child protection designated person will always notify the pupil's parents of any concerns or incidents.

Sexting

'Sexting' is one of a number of risk-taking behaviours associated with the use of digital devices, social media or the internet. It is accepted that young people experiment and challenge boundaries and therefore the risks associated with 'online' activity can never be completely eliminated. However Wootton-by-Woodstock Primary School takes a pro-active approach to help students and staff to understand, assess, manage and avoid the risks associated with online activity. The school recognises its duty of care to its young people and staff who do find themselves involved in such activity as well as its responsibility to report such behaviours where legal or safeguarding boundaries are crossed.

Sexting is defined as:

Images or videos generated

- by children under the age of 18,
- or of children under the age of 18 that are of a sexual nature or are indecent.

These images are shared between young people and/or adults via a mobile phone, handheld device, computer, 'tablet' or website with people they may not even know.

Sexting is classed as illegal as it constitutes sharing and/or possessing an indecent image of a child or sharing of images without consent of an adult.

Please see Safeguarding and Child Protection, Whistleblowing, Codes of Conduct, Behaviour, Anti-bullying and Social Media policies.

Impact

Sanctions for misuse of school technology

Sanctions for pupils

Examples of misuse of school ICT can range in severity and are dealt with accordingly. They include:

• use of non-educational sites during lessons
• unauthorised use of email or mobile phones

• accidentally or deliberately corrupting or destroying other people's data or violating others' privacy
• cyber bullying
• purchasing or ordering items over the internet
• deliberately accessing, downloading or disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
• receipt or transmission of material that infringes the copyright of other people or is in breach of the Data Protection Act
• bringing the school name into disrepute

Sanctions include:
• referral to Headteacher
• contact with parents
• possible exclusion
• referral to community police officer

Sanctions for staff

These reflect the seriousness of any breach of acceptable use policies by staff members given their position of trust. These can range in severity and are dealt with accordingly. They include:

Minor infringements –

These are minor breaches of the school's acceptable use policy which amount to misconduct and will be dealt with internally by the Headteacher.
• excessive use of internet for personal activities not connected to professional development
• use of personal data storage media without carrying out virus checks
• any behaviour on the internet that compromises professional standing in the school and community
• sharing or disclosing passwords
• breaching copyright or licence by installing unlicensed software

Major infringements –

These are deliberate actions that undermine safety and call into question the person's suitability to work with children. They represent gross misconduct and include:
• serious misuse or deliberate damage to any school computer hardware or software, e.g. deleting files, downloading unsuitable applications
• a deliberate attempt to breach data protection or computer security
• deliberately accessing, downloading or disseminating material deemed offensive, obscene, defamatory, racist, homophobic or violent
• receipt or transmission of material that infringes the copyright of other people or is in breach of the Data Protection Act
• bringing the school name into disrepute

Sanctions include:
• referral to the Headteacher
• referral to Oxfordshire's e-safety officer
• removal of equipment
• suspension pending investigation
• disciplinary action in line with school policies
• referral to police
• dismissal

	Staff and other Adults			Students / Pupils				
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	x							x
Use of mobile phones in lessons				x				x
Use of mobile phones in social time		x						x
Taking photos on mobile phones / cameras				x				x
Use of other mobile devices e.g. tablets, gaming devices				x				x
Use of personal email addresses in school, or on school network				x				x
Use of school email for personal emails				x				x
Use of messaging apps				x				x
Use of social media				x				x
Use of blogs				x				x

Monitoring and Evaluation

The school monitors and evaluates on a continuous basis through the following:

- Lesson observations and the quality of teaching
- Work sampling
- The quality and effectiveness of long, medium and short term planning
- The quality and consistency of assessing and learning
- The quality of resources to support learning
- The Head's records
- Governing body monitoring
- The number of recorded incidents
- Behaviour management plans

Professional Development

Members of staff and other adults working in the school must attend Child Protection and Safeguarding training annually as well as other relevant INSET that allow professional development to take place.

Spiritual, Moral, Social and Cultural

E-safety is a large strand of the SMSC provision for computing. The teaching of e-safety enables children and adults to gain a deeper understanding of the moral responsibility of using the internet. It prepares children for the challenge of living and learning in a technologically enriched, increasingly inter connected world; increasing awareness of the moral dilemmas created by technological advances and establishing boundaries in society by considering what is acceptable.

Equality and Access

We reflect and promote a child's key rights irrespective of irrespective of religion or belief, race, nationality, ethnicity, gender, sexual orientation, age, ability or disability, opinion or family background.
All children have equal access to opportunities in computing and have the right to access computing without the fear of risk. They have the right to experience, enjoy and express themselves in computing.
See Equality and Access, SEND, and Inclusion policies

Health and Safety

Please see Health and Safety Policy.

Wootton-by-Woodstock

ODST Oxford Diocesan Schools Trust

Pupil ICT Acceptable Use Policy Agreement – for Foundation/KS1 Pupils

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers / tablets
- I will only use activities that a teacher or suitable adult has told or allowed me to use
- I will take care of the computer and other equipment
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong
- I will tell a teacher or suitable adult if I see something that upsets me on the screen
- I know that if I break the rules I might not be allowed to use a computer / tablet

Signed (child):…….

Wootton-by-Woodstock

ODST Oxford Diocesan Schools Trust

Pupil ICT Acceptable Use Policy Agreement - for KS2 Pupils

I understand that I must use school IT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.

For my own personal safety:

- I understand that the *school* will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school systems and devices are intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- I will not make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the school systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube).

I will act as I expect others to act toward me:

- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to bypass the filtering/security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person/organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.
- I will only use social media sites with permission and at the times that are allowed

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

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I may lose access to the school network, receive other sanctions and my teacher may contact my parents. In the event of illegal activities this may involve the police.

I have read and understand the above and agree to follow these guidelines when I use the *school* systems and devices (both in and out of school)

Name of Pupil: .....

Group / Class: .....

Signed: .....

Date: .....

Wootton-by-Woodstock

ODST Oxford Diocesan Schools Trust

Parent/Carer ICT Acceptable Use Policy Agreement

As the parent / carer of the below pupil, I give permission for my son / daughter to have access to the internet and to ICT systems at school.

I know that my son / daughter has signed an Acceptable Use Agreement and has received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that 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 systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

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

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.

Parent / Carers Name: .....

Date: ……

Pupil Name: .....

E-Safety Incident Report Form

Wootton-By-Woodstock Primary School		
Your name:	Your position:	Date and time of incident:
Details of e-safety incident		
Date and time of incident:		
Where did the incident occur? i.e. at school or at home		
Who was involved in the incident? Child/young person ☐ Name of child …… Staff member/volunteer ☐ Name of staff member/volunteer …… Other ☐ Please specify …….		
Description of incident (including device used, IP addresses, relevant user names and programmes used)		

Wootton-by-Woodstock

ODST Oxford Diocesan Schools Trust

Action taken ☐ Incident reported to Headteacher/Safeguarding Lead/Deputy Safeguarding Lead ☐ Record of Concern form completed ☐ Advice sought from MASH/LCSS ☐ Incident reported to Broadband service provider ☐ Incident reported to the police ☐ E-safety policy to be reviewed/amended ☐ Disciplinary action to be taken …….. ☐ Other ……..
Outcome of investigation

Signed …….. (reporter)

Date ……..

Signed …… (Headteacher/ Safeguarding Lead)

Date ……