Online Safety

Contents

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

2. Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying 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.

This policy complies with our funding agreement and articles of association.

3. Roles and responsibilities

3.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governor who oversees safeguarding, and therefore online safety, is James Shanley.

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)

3.2 The headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The designated safeguarding lead

Details of the school's DSL and deputies are set out in our child protection and safeguarding policy as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the SLT in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the SLT, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board

This list is not intended to be exhaustive.

3.4 The ICT manager

The ICT manager is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems at least on a monthly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Working with the DSL or their deputies to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy

- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school Behaviour and Discipline Policy

This list is not intended to be exhaustive.

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- Working with the DSL or their deputies to ensure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2)

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? - UK Safer Internet Centre
- Hot topics - Childnet International
- Parent factsheet - Childnet International
- Healthy relationships – Disrespect Nobody

3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3).

4. Educating pupils about online safety

The use of technology can bring huge benefits to all pupils at Forest Way School, educationally, socially and to enable them to lead as full a life as possible. It is vital that we educate our pupils to use the technology and online services in a manner that helps to protect them from harm and ensures their safety and wellbeing.

We want our pupils to be able to use technology and online services as safely and independently as they can, in readiness for life beyond school. The school's scheme of work is progressive, building upon previous learning, to allow pupils to learn about Online Safety in a manner that is appropriate to both their level of online usage and their level of understanding.

The strands covered by the Scheme of Work are:

Online relationships	This strand teaches and encourages pupils to be good Digital Citizens. Using online services responsibly and in a way that is kind and beneficial to other users.
Online bullying	This helps to prepare the pupils for the fact that not everything or everyone they encounter in the online world will be kind to them and that sometimes they may encounter people or situations that can upset them. It teaches them how to deal with these situations when they arise and also what to do if they see it happening to somebody else.
Reliability of information	Pupils are taught to understand that not everything they read or see online is true or helpful. They are given strategies to help them decide what information to trust and

	also the implications of them sharing something that is not true. Pupils are also taught about fraud and learn strategies to help them avoid becoming victims of fraud.
Online reputation	In an age of social media, pupils are taught about the implications of sharing things online and how this may harm them in ways they might not foresee.
Privacy and security	This strand teaches the pupils about the importance of keeping their personal details and access to services private and secure.
Health and wellbeing	At a time when technical devices are almost ubiquitous, pupils are taught about responsible use and the implications to their health and wellbeing if devices are used too often and for too long.

The scheme of work shows progression through an understanding of Online Safety. It contains 6 areas of progression with statements in progressive order for each of the 6 strands of Online Safety, moving towards a high level of understanding that will support the pupils whether they continue to be supported, live independently or move into the world of employment. This scheme of work draws upon the National Curriculum in England, the Education for a Connected World Framework, the Government's "Teaching online safety in schools" guidance as well as guidance from Online Safety charities such at the Safer Internet Centre, The NSPCC and ChildNet.

The safe use of social media and the internet will also be covered in other subjects where relevant.

5. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents.

Online safety will also be covered during parents' evenings.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or any Deputy DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The school will also provide information on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school Behaviour and Discipline Policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation and the school's COVID-19 risk assessment.
Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

7. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (Appendices 1 and 2). 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, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the Acceptable Use Agreements in Appendices 1 and 2.

8. Pupils using mobile devices in school

Pupils may bring mobile devices into school but should only use them when given permission to do so.

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see Appendix 1).

9. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure and ensure all use complies with the school's Adult Acceptable Use Policy (see Appendix 2).

The computers, electronic media and services provided by the school are primarily for educational use to assist staff in the performance of their job. Staff, learners, and parents are expected to demonstrate a sense of responsibility and not abuse this privilege.

Any devices provided by the school for the purpose of remote learning belong to the school and must be used under the supervision of an adult in accordance with the Acceptable Use Policy.

10. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our Acceptable Use Policy for Pupils and the Behaviour and Discipline Policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the Staff Attendance, Conduct and Grievance Policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

12. Remote Learning

During the national lockdowns during the Covid-19 pandemic, Forest Way, like most schools, stayed open throughout the period to support its most vulnerable pupils and those of key workers. As all students at Forest Way have an EHCP, and are by definition a vulnerable group, this aspiration stays in place. However, during the lockdowns, many pupils are not in school and it is also important to plan for the potential closure of Bubbles or a whole school closure that ensures the minimum disruption to learning and the maintenance of effective safeguarding.

In the case of remote learning, the provisions of this policy must be applied in conjunction with those in the Remote Learning Policy.

12.1 "Live" Lessons and Pre-recorded Video

The school uses Microsoft Teams to provide remote learning for those children not in school both through the sharing of documents and pre-recorded video as well as the use of the virtual meeting functionality to provide "live lessons". When pre-recording videos or attending "live" lessons or meetings, and in line with the Remote Learning Policy, staff will ensure they adhere to the following:

- Attending "live" virtual meetings or "live" lessons with parents and/or pupils –
    - Staff will be appropriately dressed as per the school's dress code
    - If TEAMs calls are made from a home setting than the staff members location within the home should be in suitably professional setting with the background blurred.
    - To safeguard both children, staff and parents the TEAMs recording facility should not be used.
    - Within school, the virtual lesson will be conducted in a room with another adult in place.
    - A parent or carer must be present during the live meeting.

12.2 Security of Remote Learning

- Learners have individual usernames and passwords for security.
- Users should not give out their username or passwords to anyone.

- Children and staff must not disclose any password or login name given to anyone or allow anyone else to use a personal account.
- Children and staff must not attempt to gain access to the school network or any internet resource by using somebody else's account name or password.
- Staff and children must ensure terminals. Laptops or devices are logged off when left unattended.
- Children are only allocated to Teams in which they are grouped in school, e.g. their class and ability group. They are not able to see any other groups.
- Please be aware that all the group members within each Team are able to see comments made, including learners, teachers and parents. A team may have multiple teachers as group members for monitoring and management purposes.

12.3 Reporting of Online Safety incidents during home learning

Any concerns or incidents related to Online Safety that arise during a home learning period must be reported to the Headteacher immediately and will be dealt with in line with the school's Child Protection Policy. Any material deemed as inappropriate content will be removed at the school's discretion and will be dealt with in accordance with the school's Child Protection Policy and Behaviour and Discipline Policy.

13. Monitoring arrangements

The DSL and their deputies log behaviour and safeguarding issues related to online safety in accordance with the schools' Child Protection Policy.

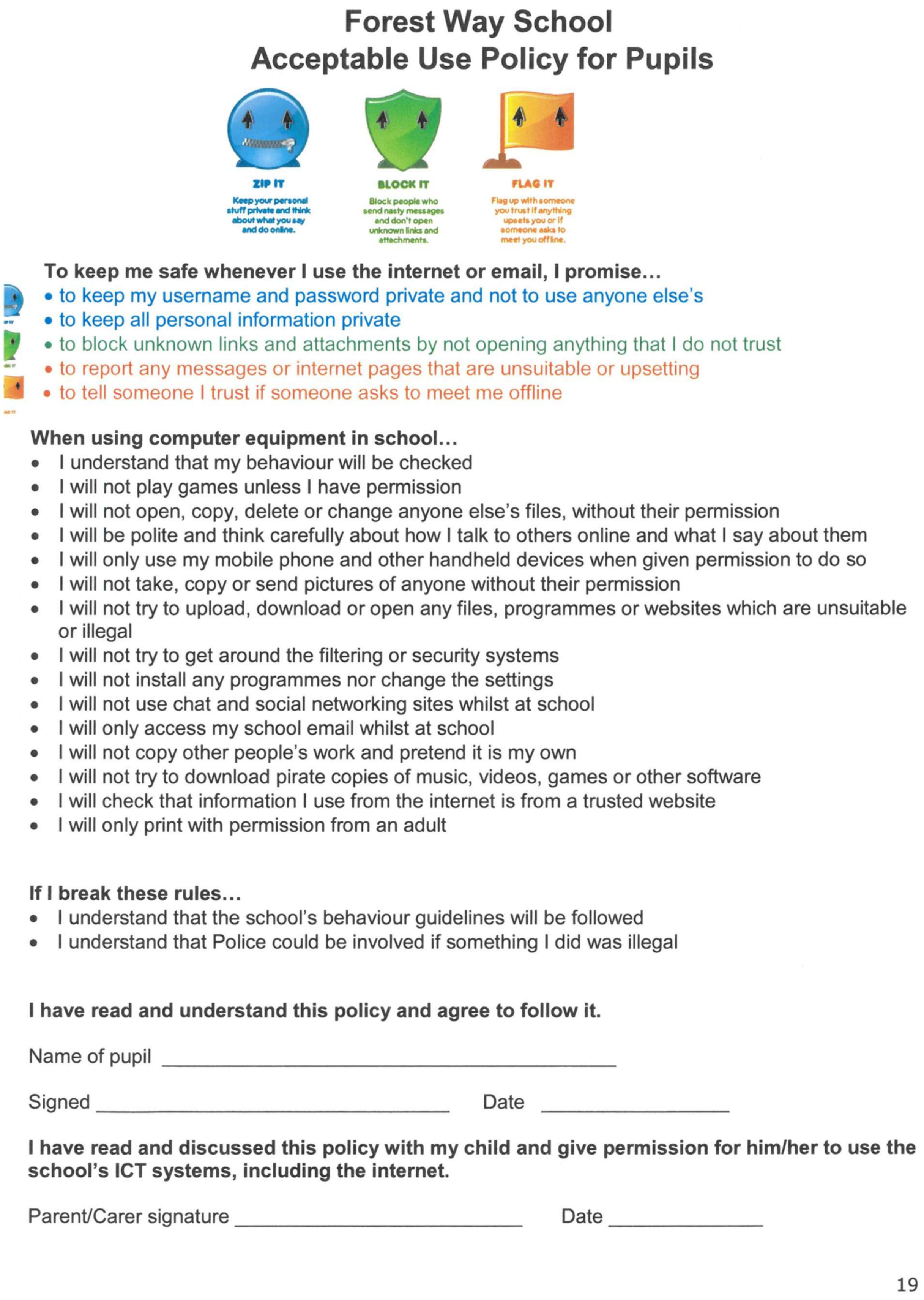
This policy will be reviewed annually by the headteacher. At every review, the policy will be shared with the governing board.

14. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour and Discipline Policy
- Staff disciplinary procedures
- Data Protection/Security and GDPR Policy
- Complaints procedure
- ICT and internet acceptable use policy

Appendix 1: Forest Way School Acceptable Use Policy for Pupils



Forest Way School
Acceptable Use Policy for Pupils

ZIP IT

Keep your personal stuff private and think about what you say and do online.

BLOCK IT

Block people who send nasty messages and don't open unknown links and attachments.

FLAG IT

Flag up with someone you trust if anything upsets you or if someone asks to meet you offline.

To keep me safe whenever I use the internet or email, I promise…

- to keep my username and password private and not to use anyone else's
- to keep all personal information private
- to block unknown links and attachments by not opening anything that I do not trust
- to report any messages or internet pages that are unsuitable or upsetting
- to tell someone I trust if someone asks to meet me offline

When using computer equipment in school…

- I understand that my behaviour will be checked
- I will not play games unless I have permission
- I will not open, copy, delete or change anyone else's files, without their permission
- I will be polite and think carefully about how I talk to others online and what I say about them
- I will only use my mobile phone and other handheld devices when given permission to do so
- I will not take, copy or send pictures of anyone without their permission
- I will not try to upload, download or open any files, programmes or websites which are unsuitable or illegal
- I will not try to get around the filtering or security systems
- I will not install any programmes nor change the settings
- I will not use chat and social networking sites whilst at school
- I will only access my school email whilst at school
- I will not copy other people's work and pretend it is my own
- I will not try to download pirate copies of music, videos, games or other software
- I will check that information I use from the internet is from a trusted website
- I will only print with permission from an adult

If I break these rules…

- I understand that the school's behaviour guidelines will be followed
- I understand that Police could be involved if something I did was illegal

I have read and understand this policy and agree to follow it.

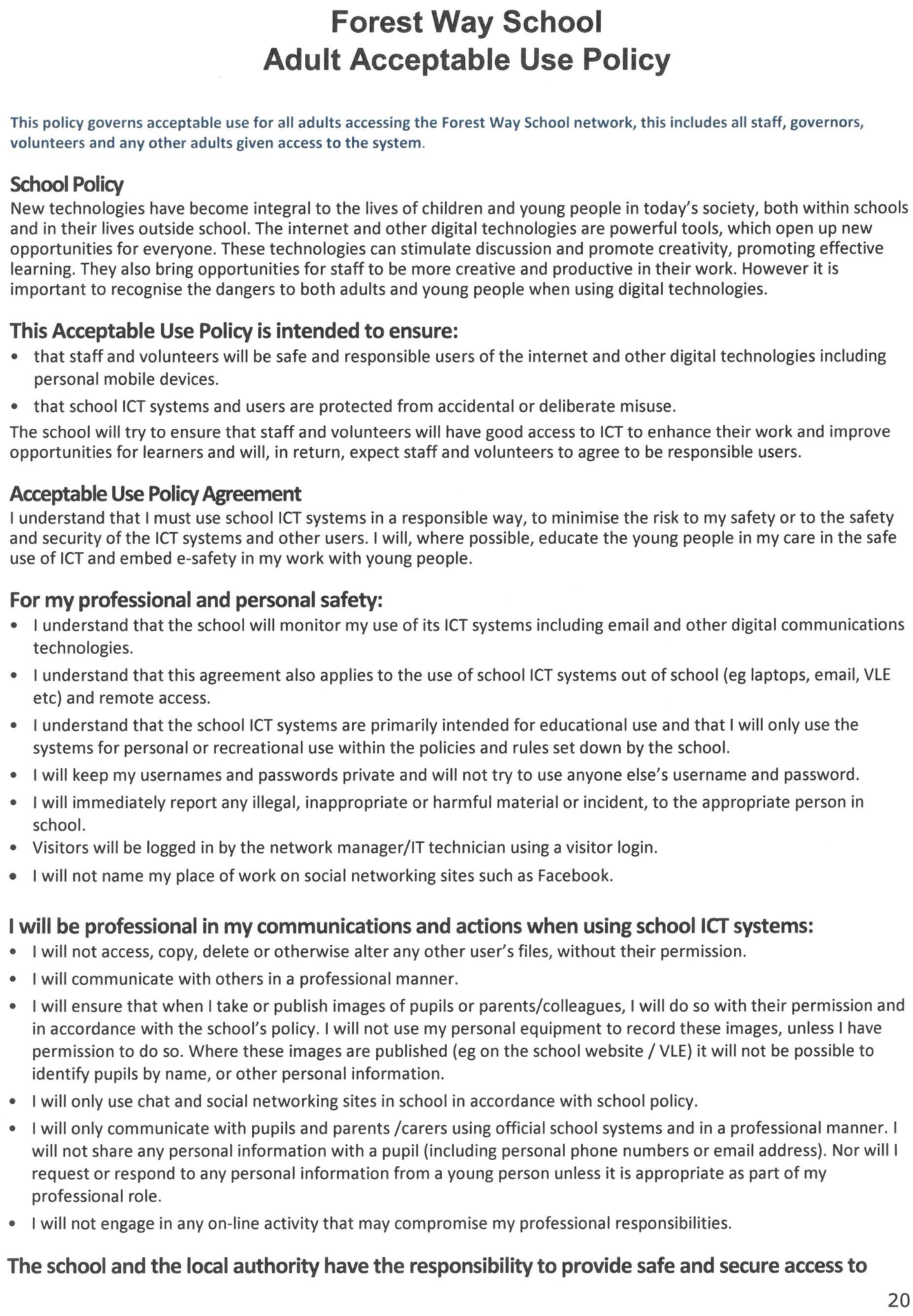
Name of pupil ____

Signed _______________________________ Date ________________

I have read and discussed this policy with my child and give permission for him/her to use the school's ICT systems, including the internet.

Parent/Carer signature __________________________ Date ______________

Appendix 2: Forest Way School Adult Acceptable Use Policy



Forest Way School
Adult Acceptable Use Policy

This policy governs acceptable use for all adults accessing the Forest Way School network, this includes all staff, governors, volunteers and any other adults given access to the system.

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion and promote creativity, promoting effective learning. They also bring opportunities for staff to be more creative and productive in their work. However it is important to recognise the dangers to both adults and young people when using digital technologies.

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be safe and responsible users of the internet and other digital technologies including personal mobile devices.
- that school ICT systems and users are protected from accidental or deliberate misuse.

The school will try to ensure that staff and volunteers will have good access to ICT to enhance their work and improve opportunities for learners and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to minimise the risk to my safety or to the safety and security of the ICT systems and other users. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of its ICT systems including email and other digital communications technologies.
- I understand that this agreement also applies to the use of school ICT systems out of school (eg laptops, email, VLE etc) and remote access.
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will keep my usernames and passwords private and will not try to use anyone else's username and password.
- I will immediately report any illegal, inappropriate or harmful material or incident, to the appropriate person in school.
- Visitors will be logged in by the network manager/IT technician using a visitor login.
- I will not name my place of work on social networking sites such as Facebook.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, delete or otherwise alter any other user's files, without their permission.
- I will communicate with others in a professional manner.
- I will ensure that when I take or publish images of pupils or parents/colleagues, I will do so with their permission and in accordance with the school's policy. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (eg on the school website / VLE) it will not be possible to identify pupils by name, or other personal information.
- I will only use chat and social networking sites in school in accordance with school policy.
- I will only communicate with pupils and parents /carers using official school systems and in a professional manner. I will not share any personal information with a pupil (including personal phone numbers or email address). Nor will I request or respond to any personal information from a young person unless it is appropriate as part of my professional role.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to

technologies:

- All Forest Way School data should only be stored on the Forest Way School Network or encrypted devices provided by school.
- Forest Way School does not allow the use of Cloud storage for users of its network. (Forest Way does utilise Cloud backups managed by the Network Manager/IT technician.)
- When I use my personal hand held / non Forest Way School devices in school (PDAs / laptops / mobile phones / USB devices/ tablets etc), I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that I am given permission to connect to school ICT systems, they are protected by up to date anti-virus software and are free from viruses. I will not connect any personal devices to the school network without relevant permission.
- I will not use personal email addresses on the school ICT systems.
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will not name my place of work on social networking sites such as Facebook.
- The school provides adequate data storage and remote access therefore e-mails should not contain images of pupils or personal or confidential information of staff or pupils.
- I will ensure that my data is available for regular backups (synchronising documents with server). The responsibility for data backup and disaster recovery will rest with the IT support manager.
- I will not try to upload, download or access any material which is illegal or inappropriate or may cause harm or distress to others on school equipment or on personal equipment on school premises (eg child sexual abuse images, criminally racist material, adult pornography etc). I will not try to use any programmes or software that might allow me to bypass the filtering / security systems intended to prevent access to such materials.
- Unless I have permission, I will not try to 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 install or attempt to install programmes of any type on school systems, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Data Protection Policy. Where personal data is electronically transferred outside the secure school network, it must be encrypted.
- Access to management information systems will be tightly monitored and data will not be shared under any circumstances due to the sensitivity of the data.
- I will use the printers and photocopiers appropriately only printing when necessary and for school use only.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

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

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.
- I will not bring the school into disrepute through the use of social networking sites such as Twitter, Google Plus and Facebook. I will not post photos, videos, comments or information related to the school or members of staff.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action and in the event of illegal activities, the involvement of the police.

I have read and understand the above and agree to use the school ICT systems both in and out of school and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Name ____

Signed ____________________________ Date _____________________

Appendix 3: online safety training needs – self audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	**Date**:
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in school?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	