Contents

Acceptable Use Policy
Federation of St. Peter’s CofE (VA) Elwick and Hart Primary Schools

1. Rationale

Our school’s vision is to ensure that we deliver high standards of teaching and learning by supporting the effective use of ICT.

This Acceptable Use Policy (AUP) has been created by our school governors and senior managers and approved by the whole school community through a process of consultation. The purpose of this policy is to ensure the school network is operated safely and all users of ICT are safe and stands alongside other school policies such as our computing policy. It also contributes to ensuring all pupils are safe online, safe from bullying and discrimination; safe from crime and anti-social behaviour in and out of school

This AUP refers to our school ICT network and to the use of mobile technologies within it. It explains the behaviours, which are acceptable and unacceptable, with regard to use of ICT within our school. This policy combines and works in conjunction with the *Northern Grid for Learning Acceptable Use Policy* to which our school adheres.

Our AUP applies to:

- All employees in our school;
- Pupils;
- Parents;
- Governors;
- Visitors;
- outside agencies.

It must be fully complied with at all times. All users of the school network should note that it is monitored on a regular basis. Any person who is found to have misused the school system or not followed our AUP could face the following consequences:

- Temporary or permanent withdrawal from the school system
- Suspension or exclusion from the school
- Disciplinary action
- In the most serious cases legal action may also be taken.

2. School Philosophy/Culture

Our school ensures that all pupils and adults are treated equally and with respect.

3. School Organisation

Our network, systems and staff are organised to maintain the most secure environment possible.
3.1 We have an E-Safety Co-ordinator who reviews and advises on our policies.

The roles and responsibilities of each person involved are outlined below.

3.2. Executive Head Teacher

The Executive Head Teacher takes ultimate responsibility for internet safety issues within the school, while delegating day-to-day responsibility to the E-Safety Coordinator. They support the work of the E-Safety Coordinator by:

- Ensuring that the E-Safety Coordinator and members of the school E-Safety Teams are given appropriate time, support and authority to carry out their duties effectively.
- Ensuring that developments at local and partnership level are communicated to the Teams.
- Supporting the E-Safety Coordinator in creating an internet safety culture within the school, including speaking to staff and pupils in support of the programme.
- Ensuring that the governing body is informed of the issues and the policies.
- Ensuring that appropriate funding is allocated to support internet safety activities throughout the school, for both the technical infrastructure and Inset training.
- Promoting internet safety across the curriculum.

3.3. E-Safety Coordinator

The primary responsibility of the E-Safety coordinator is to establish and maintain a safe ICT learning environment within the school. They do this by:

- Leading the school E-Safety and Policy review and development.
- Working with staff and the Head Teacher to develop, and review, appropriate internet safety policies and procedures.
- Leading on the development of management protocols so that any incidents in which internet safety is breached are responded to in an appropriate and consistent manner.
- Leading in the creation of a staff professional development programme that addresses both the benefits and risks of communication technologies:
  - Produce written information provided with a staff use agreement, an internet safety manual or handbook for staff
  - Give regular presentations at staff meetings, and hands-on training sessions on practical aspects of internet safety.
  - Ensure staff are aware that they have professional responsibilities for pupils' safety in this area.
- Leading in the creation of an internet safety education programme for pupils, maintaining an overview of activities across the school, and supporting staff with information and resources as appropriate.
- Developing a parental awareness programme.
- Maintaining a log of all incidents relating to internet safety in school.
- Making recommendations for review of policy and technological solutions on the basis of analysis of logs and emerging trends.

- Meeting regularly with the Head Teacher to discuss internet safety issues and review progress.
- Updating the governing body on current internet safety issues, in conjunction with the Head Teacher.
- Liaising with outside agencies, which may include the LA, local schools, city learning centre, or national agencies, as appropriate.
- Developing a cycle of creation, maintenance, ongoing review, modification and reporting of all E-Safety safety policies and practices.

4. Governing Body

Our Governing Body has statutory responsibilities for child protection and health and safety, and elements of these include internet safety. Our Safeguarding Governor has responsibility for ensuring that internet safety is included as part of the regular review of child protection and health and safety policies. Our Governing Body is also involved in:

- Developing an awareness of the issues and risks of using ICT in schools, alongside the benefits, particularly with regard to the internet and other communications technologies.
- Developing an understanding of existing school policies, systems and procedures for maintaining a safe ICT learning environment and supporting the Head Teacher and E-Safety Coordinator in implementing these, including ensuring access to relevant training for all school staff.
- Supporting the Head Teacher and E-Safety Coordinator in developing an appropriate strategy and plan for dealing with the media should serious incidents occur. In such an instance, it is likely that the chair of the governing body will be approached by the press for comment.
- Ensuring that appropriate funding is authorised for internet safety solutions, training and other activities as recommended by the Head Teacher and E-Safety Coordinator as part of the wider remit of the governing body with regard to school budgets.
- Promoting internet safety to parents, and providing updates on internet safety policies within the statutory 'security' section of the annual report.

4.5. Network manager (ICT Technician)

Our network manager has an important role to play in establishing and maintaining a safe ICT learning environment for the school. This role is bought into through ITSS. The responsibilities for the safe upkeep of the network involve the Network Manager:

- Acting as a key member of the school's E-Safety team, supporting the E-Safety Coordinator in the development and maintenance of appropriate policies and procedures through technical information and advice.
- Providing a technical infrastructure to support internet safety practices, this includes;
    - Ensuring that appropriate and effective electronic security systems are in place, such as filtering, monitoring and firewall technology, and virus protection supported by regular and thorough monitoring of computer networks.
    - Documenting the location of all internet-accessible computers within the school.
    - Advising on the positioning of internet-enabled computers within the school to allow easy supervision of pupils' work, and hence discourage breaches of AUPs.
    - Ensuring that staff workroom computers are secure.
    - Ensuring that appropriate processes and procedures are in place for responding to the discovery of illegal materials on the school's network, or the suspicion that such materials exist.
    - Ensuring that appropriate processes and procedures are in place for responding to the discovery of inappropriate but legal materials on the school's network.
- Reporting network breaches of acceptable use of ICT facilities to the internet safety co-ordinator and other staff members as appropriate.

- Maintaining a high level of professional conduct in their own internet use both within and outside school.

4.6. Classroom Teachers and Teaching Assistants

The teaching team will probably be the first point of contact in dealing with incidents of ICT misuse or abuse and may be required to act as mediators for ICT-related incidents which occur inside and outside school, such as bullying within chat rooms. They follow the procedures outlined in this AUP and are involved in:

- Developing and maintaining knowledge of internet safety issues, particularly with regard to how they might affect children.
- Implementing school AUP through effective classroom practice.
- Ensuring any instances of ICT misuse, whether accidental or deliberate, are dealt with through the proper channels, reporting to the E-Safety Coordinator in line with our school AUP.
- Ensuring that they provide the necessary support to pupils who experience problems when using the internet, working with the E-Safety Coordinator, SENDCO and/or child protection liaison officers as appropriate.
- Planning classroom use of the internet and ICT facilities to ensure that internet safety is not compromised; evaluating websites in advance of classroom use (for example, by bookmarking and caching sites) and ensuring that school filtering levels provide appropriate protection for topics being studied.
- Embedding teaching of internet safety messages within curriculum areas wherever possible.
- Maintaining an appropriate level of professional conduct in their own internet use both within and outside school, including the conduct of posts on their own social media. This also includes comments made on their own social media posts.

4.7. Special Educational Needs Coordinator (SENDCO)

Primarily, our SENDCO considers the needs of all pupils, and whether our internet safety programme is appropriate to the needs of those pupils with special educational needs, or whether additional tailored materials are required. As such they are involved in:

- Developing and maintaining knowledge of internet safety issues, particularly with regard to how they might affect children and young people.
- Developing and maintaining additional policies and internet safety materials, in conjunction with the E-Safety Coordinator and the E-Safety Teams, tailored to the special educational needs of pupils.
- Liaising with parents of pupils with special educational needs to ensure that they are aware of the internet safety issues their children may encounter outside school, and the ways in which they might support them.
- Co-operating with the child protection liaison officer, as necessary liaising with other individuals and organisations, to ensure that those pupils being educated away from school premises still benefit from a safe ICT learning environment.

5. Designated Person - Child Protection

Our Designated Person (Child Protection) is the first point of contact for any internet safety issue which may compromise the wellbeing of a pupil and as such they are involved in:

- Seeking professional development on the safety issues relating to use of the internet and related technologies, and how these relate to children and young people, refreshing this knowledge on a regular basis.
- Acting as a key member of the school's E-Safety Teams, liaising with the E-Safety Coordinator on specific incidents of misuse, and providing follow-up counselling and support to both victims and perpetrators as appropriate.
- Taking a proactive role in the internet safety education of pupils.
- Developing systems and procedures for supporting and/or referring on pupils referred to them as a result of breaches of internet safety within schools.
- Developing systems and procedures for pupils who self refer, and those pupils identified as suspected 'victims' by teaching staff.
- Developing relationships with colleagues at LA level (including counsellors and guidance staff) and other organisations that can provide advice, referrals or resources on issues relating to child protection on the internet.

5.9. Pupils

Our ultimate aim is for pupils to take responsibility for their own actions when using the internet and other communications technologies, with each pupil developing a set of safe and discriminating behaviours to guide their own internet use. Responsibilities we promote are:

- Contributing to school AUP through involvement in the school's E-Safety Policy Team.
- Upholding school policies relating to acceptable use of the internet and other communications technologies.
- Developing their own set of safe and discriminating behaviours to guide them whenever they are online.
- Reporting any incidents of ICT misuse within school to a member of the teaching staff
- Seeking help or advice from a teacher or trusted adult if they experience problems when online or if they receive any content or contact which makes them feel uncomfortable in any way.
- Communicating with their parents or carers about internet safety issues, and upholding any rules for safe internet use in the home.

6. Definitions

It is important to differentiate between *inappropriate* and *illegal* use. Procedures and sanctions also vary whether the access is *deliberate* or *accidental*. It is important to be clear about which type of incident has occurred or is suspected as the procedures differ in each case.

6.1. Outline of Inappropriate Use

Inappropriate use of the network includes accessing or having possession of material that is thought to be offensive such as:

- Pornography
- Hate material
- Drug or bomb making recipes
- Sexist or racist jokes or cartoons
- Material used in a low level harassment
- Material that others may find offensive
- Defamatory, offensive, abusive, indecent or obscene
- Material used in breach of confidence, privacy, trade secrets

6.2. Outline of Unlawful or Illegal Use

Unlawful or illegal use of the network includes accessing or having possession of material that contains:

- Direct threats of physical harm
- Child abuse images
- Incitement to racial hatred or violence
- Copyrighted, trademarked and other proprietary material used without proper authorisation

These are not exclusive categories. There may be other information that is deemed to be illegal.

5. Reporting Procedures

In all cases of incidents within school it may be necessary to review policies and procedures immediately after the event to prevent further cases occurring.

5.1. Inappropriate Material

5.1.1. Procedures for reporting Accidental Access to Inappropriate Material

Despite procedures in place, it is impossible to guarantee that there will never be accidental access to inappropriate or offensive material.

Anyone who accidentally comes across inappropriate or offensive material must do the following:

1. Inform the E-Safety Coordinator (children report to class teacher who passes the information on the E-Safety Coordinator) of the incident and give the website address or details of the email received.
2. The E-Safety Coordinator will log the web address or incident, time and username in the web log book which is retained by the E-Safety Coordinator.
3. The E-Safety Coordinator will inform the Head Teacher (unless the Head Teacher is directly involved in the incident).

4. The E-Safety Coordinator will ring the Easynet school support helpdesk (Tel. 0845 333 4568) and report the web address, asking for an investigation as to whether the website should be permanently blocked.
5. If Easynet decide that the website is not sufficiently inappropriate for permanent blocking, the school will block the website via its own CachePilot and ensure the Internet History log is cleared.
6. The E-Safety Coordinator will then make a judgement call on the severity of the incident and the effect it may have had on the pupil(s) and may take further action such as convening an E-Safety Management Team meeting, informing parents, counselling the children etc.

5.1.2. Procedures for reporting Suspected Deliberate Access to Inappropriate Material

1. Anyone who suspects another person of deliberately accessing inappropriate or offensive material must do the following:
2. Report in confidence to the E-Safety Coordinator (or a senior member of the E-Safety Team if the E-Safety Coordinator is suspected) outlining reason for suspicion and details of the incident.
3. The E-Safety Coordinator will log the web address or incident, time and username in the web log book, retained by the E-Safety Coordinator.
4. The E-Safety Coordinator will inform the Head Teacher (unless the Head Teacher is directly involved in the incident).
5. The E-Safety Coordinator will ring the Easynet school support helpdesk (Tel. 0845 333 4568) and report the web address asking for an investigation as to whether the website should be permanently blocked.
6. If Easynet decide that the website is not sufficiently inappropriate for permanent blocking, the school will block the website via its own CachePilot.
7. The E-Safety Coordinator will then report to Gill Alexander, Chief Executive, who will then request that an internal RIPA form is sent, requiring Northern Grid to complete an internal investigation.
8. The E-Safety Coordinator will then make a judgement call on the severity of the incident and the effect it may have had on the pupil(s) and may take further action such as convening an E-Safety Management Team meeting, informing parents, counselling the children etc.
9. If the investigation confirms that inappropriate behaviour has occurred, the Head Teacher will follow school procedures and disciplinary proceedings may ensue on the grounds of misconduct or gross misconduct.

5.2. Unlawful or Illegal material

If you access any content including images, which you believe could be illegal it is imperative that you make no attempt to investigate the content.

5.2.1. Procedures for reporting Accidental Access to Illegal Material

Anyone who accesses the school network and who accidentally comes across illegal material should do the following:

1. Do not show anyone the content or make public the URL. If the content is an image in the body of an email under no circumstances forward the email, copy the image or show it to another person, as each of these actions constitutes an illegal offence.
2. Report the incident to the E-Safety Coordinator (children report to class teacher who passes the information on the E-Safety Coordinator)

3. The E-Safety Coordinator will then log the web address or incident, time and username in the web log book. This log reference is to protect you from any suspicion for having potential illegal material in your possession.
4. The E-Safety Coordinator will inform the Head Teacher (unless the Head Teacher is directly involved in the incident).
5. The E-Safety Coordinator will go to the Internet Watch Foundation (IWF) website at http://www.iwf.org.uk/ and click the 'Report Illegal Content' button, they will advise what will happen next and what you need to do to preserve evidence. If reporting a URL do not use copy and paste, type the URL.
6. The E-Safety Coordinator will then report to Gill Alexander, Chief Executive, who will then make sure a record of the incident is kept and follow Local Authority procedures.

5.2.2. Procedures for reporting Suspected Deliberate access to Illegal Material

Any person suspecting another of deliberate misuse or abuse of the school network should take the following action:

1. Report in confidence to the E-Safety Coordinator (or a senior member of the E-Safety Team if E-Safety Coordinator is suspected) outlining reason for suspicion and details of the incident.
2. The E-Safety Coordinator will then log the web address or incident, time and username in the web log book.This log reference is to protect you from any suspicion for having potential illegal material in your possession.
3. The E-Safety Coordinator will inform the Head Teacher (unless the Head Teacher is directly involved in the incident).
4. The E-Safety Coordinator will go to the Internet Watch Foundation (IWF) website at http://www.iwf.org.uk/ and click the 'Report Illegal Content' button, they will advise what will happen next and what you need to do to preserve evidence. If reporting a URL do not use copy and paste, type the URL.
5. The E-Safety Coordinator will then report to Gill Alexander, Chief Executive, who will then request that an internal RIPA form is sent, requiring Northern Grid to complete an internal investigation.
6. If the investigation confirms access to illegal materials or the committing of illegal acts has occurred, Northern Grid will inform the relevant authority which may be the LA or the school governing body.

In exceptional circumstances, where there are reasonable grounds to suspect that a user has committed a serious criminal offence, the police will be informed and criminal prosecution may follow.

6. School ICT Network

To ensure maximum security and maximum benefits for curriculum use it is vital that all users of the Network comply with the rules in the following sections.

6.1. Security of the Network and CachePilot

The school Network and associated services may be used for lawful purposes only.

You are prohibited from storing, distributing, transmitting or permitting the storage distribution or transmission (whether intentionally or otherwise) of, any unlawful or illegal material through the network.

As a user of our Network you agree not to use it to send or receive materials or data, which is deemed inappropriate.

All PCs on the school network are authenticated and directed through the CachePilot. The main purpose of this is to set up lists of approved sites that are suitable for viewing in accordance with the AUP. However it is impossible to prevent all inappropriate material from being accessed even in such a secure environment. Attempts to bypass the CachePilot authentication may result in sanctions.

The Network Manager (ITSS) will up-date virus protection regularly on the school network and perform a regular back-up of the data stored.

6.2. Passwords

The following rules must be followed regarding passwords to ensure the school network is secure and monitoring can effectively take place.

- Each child and adult working within the school must log on using their own password.
- Don’t lose or give your password to anyone (if your password is lost or someone finds out what your password is inform the E-safety team)
- Always use your own password
- Always log off the computer to prevent unauthorised access.
- Change passwords regularly (staff)
- Never leave Administration / Superuser accounts logged on or unattended at any time.
- Any supply teachers or visitors to the school must log onto the system as a Guest only and a record will be kept of who is using each unique Guest password.

6.3. Software and downloads

- All users of the network must virus check any USB device storage devices before using on the network.
- All users are prohibited from installing software onto the network from a CD-ROM or other device without permission from the ICT Co-ordinator.
- All users are prohibited from downloading software from the Internet without permission from the ICT Co-ordinator.
- Copyright and intellectual property rights must be respected when downloading from the internet.

6.4. Email

Only e-mails which are filtered against spam and viruses are permitted to be opened in school. All emails sent from school must include the school disclaimer: This email is sent on behalf of Federation of St. Peter’s Elwick CofE (VA) and Hart Primary Schools and is strictly confidential and intended solely for the addressee[s]. It may contain personal and confidential information and as such may be protected by the Data Protection Act 1998. If you are not the intended recipient of this email you must: (i) not disclose, copy or distribute its contents to any other person nor use its contents in any way or you may be acting unlawfully (ii) contact St. Peter’s Elwick CofE (VA) or Hart Primary School immediately on 01429 274904 or 273283 quoting the name of the sender and the addressee then delete it from your system. You should scan attachments (if any) for viruses.

Users are responsible for e-mail they send and for contacts made and should be aware that these are open to be read and should be treated as public. e-mail should be written carefully and politely and should never contain anything which is likely to cause annoyance, inconvenience or needless anxiety. When sending an e-mail using the school network the use of abusive language (swearing) is strictly forbidden. Make sure nothing in the messages could be interpreted as libellous. Racist comments must never be sent using e-mail or any racist e-mails forwarded using the schools network. Online bullying using e-mail and online messenger services will not be tolerated.

E-mail attachments should only be opened if the source is known and trusted. The opening of spam e-mails should be avoided as these often carry viruses that may damage the school network and internet sever. Any e-mails that appear to be spam should be deleted rather than opening. Spam e-mails, promotional or advertising material and chain mails must never be sent or forwarded from any computer within school.

E-mail addresses must never be broadcasted publicly and children are not permitted under any circumstances to e-mail a member of staff using their personal e-mail address. When emailing parents school email addresses must be used, rather than personal email addresses.

Pupils must never give out personal details such as name, address, age or telephone number. Any unsuitable communications received must be reported to a member of staff immediately.

6.5. Uploading images/videos

All children need parental permission to have photographs or videos published electronically or in a public area even if they are unidentifiable. Photographs uploaded onto school website or social media must be carefully vetted to ensure that they are appropriate, including any background images. It is the responsibility of the adult uploading the photographs to check for parental permission on the appropriate paperwork stored in school.

No photos or videos which include nudity or inappropriate actions are permitted to be downloaded under any circumstance as this constitutes misuse.

6.6. Network Protocol

- School computer and Internet use must be appropriate to a pupil's education or to staff professional activity.
- Respect other people’s material and do not corrupt, interfere with or destroy them. Do not open other people’s files without express permission.
- When working with SIMS or any other personal data ensure that the data is secure.

6.7. Internet Usage

Pupils must be supervised at all times when using the internet.
Activities should be planned so ‘open searching is kept to a minimum. The facility for caching sites should be used prior to using the internet with pupils.
When searching the internet with pupils ‘child safe’ search engines should be used such as:

http://www.bbc.co.uk/cbbc/search
http://www.ajkids.com
http://www.kidsclick.org
http://www.yahooligans.com

The use of public chat rooms and messaging systems (e.g. ICQ, MSN Messenger) is not allowed.

Use the internet for personal financial gain, gambling, political purposes or advertising is forbidden.

6.8. Mobile devices

The term mobile devices refers to some of the following which are allowed to be used in school:

- PDAs
- Laptops (school and personal)
- USB portable memory devices (pens/stick drives)
- Digital Cameras
- Video Cameras
- Dictaphones
- Mobile Phones

This is not an extensive list and the list will be reviewed annually.

Laptops are monitored for internet access via the school network and this policy applies to the use of laptops both inside and outside of school. If schools decide that laptops may be used by other members of the family, we recommend that staff have separate family user logons.

Flash drives can be used in each computer within the school. The school network scans the drive each time it is inserted to the computer for viruses. Any personal/pupil data must be stored on secure USB devices.

Adults may use mobile phones in school but these must be used in break times in appropriate areas of the school, e.g. staff room. Photographs of children must not be taken on personal devices.

Images of the children and staff stored on any mobile device must be carefully monitored. Such mobile devices should be stored in a safe place and images of children/staff from the school must be saved or deleted before the device is used by another person. The saved images must also be stored in a safe place to prevent unauthorised access i.e. locked drawer, cupboard, safe or password protected mobile device. No images of the children should be taken without parental consent using any mobile device. No images of children should be taken on any personal devices.

Possible Sanctions for misuse

Any person who is found to have misused the school system or not followed the schools' Acceptable Use Policy could face the following consequences.

- Temporary or permanent withdrawal from the school system
- Suspension or exclusion from the school
- Disciplinary action
- In the most serious cases legal action may also be taken.

7. Policy Review

This policy will be reviewed annually by the E-Safety Co-ordinator and SLT, and under guidance from the LA and Northern Grid for Learning. The policy may also be reviewed in response to technological advances and in the event of the need to change procedures and practices within the policy.