Finedon Schools

Online Safety and Acceptable Use Policy

The Online Safety Lead for Finedon Schools is:

Lucy Sadler.

The Designated Persons for Child Protection are:

Joanne Lloyd-Williams (Head Teacher)
Caroline Jewell (PSA)
Karen Ellis (SENDCo)
Lucy Sadler (Deputy Head Teacher)
Felicity Pettitt (Assistant Head Teacher).

1. What is an AUP (Acceptable Use Policy)?

This Acceptable Use Policy sets out the roles, responsibilities and procedures for the acceptable, safe and responsible use of all technologies to safeguard adults, children and young people within our school. The policy recognises the ever changing nature of emerging technologies within the curriculum and media and highlights the need for regular review to incorporate development within ICT. At present the internet technologies used extensively by young people in both home and school environments include:

- School websites/blogs
- Social Networking
- Gaming/forums on Xbox Live etc.
- Music Downloading
- Mobile phones with wireless connectivity
- Email and Instant Messaging
- Office 365
- Skype
- Video Broadcasting
- Apple/Windows apps

This policy provides support and guidance to parents/carers and the wider community (where appropriate) for the safe and responsible use of these technologies beyond the school or educational setting. It also explains procedures for any unacceptable use of these technologies by children or young people, and refers to school disciplinary procedures for staff.

2. Why have an AUP?

The use of the internet as a tool to develop learning and understanding has become an integral part of school and home life. There are always going to be risks to using any form of communication which lies within the public domain. Therefore, it is imperative that there are clear rules, procedures and guidelines to minimise those risks whilst children access these technologies.

The risks include:

- Spam and other inappropriate e-mail.
- Online grooming.
- Illegal activities of downloading or copying any copyright materials and file-sharing via the internet or any mobile device.
- Viruses.
- Cyberbullying.
- Sexting-the sending of indecent personal images, videos or text via mobile phones for private viewing.
- On-line content which is abusive or pornographic.
- Radicalisation and other religious movements.
- Social and emotional effects of an increased use of technology.

It is also important that adults are clear about the procedures, for example, only contacting children and young people about homework via a school e-mail address, not a personal one, so that they are also safeguarded from misunderstandings or allegations through a lack of knowledge of potential risks. Where possible, another member of staff should be copied into emails to also reduce risks. There is also a responsibility to educate parents about the risks and how this is managed inside of school, along with what they can do at home to help safeguard their child.

As part of the 'Every Child Matters' agenda set out by the government, the Education Act 2004 and the Children's Act, it is the duty of schools to ensure that children and young people are protected from potential harm both within and beyond the school environment. Every effort will be made to safeguard against all risks, however it is likely that we will never be able to completely eliminate them. Any incidents that do arise will be dealt with quickly and according to policy to ensure children and young people continue to be protected.

3. Aims

- To emphasise the need to educate staff, children and young people about the pros and cons of using new technologies both within and outside school or other educational settings.
- To provide safeguards and rules for acceptable use to guide all users, whether staff or student, in their online experiences.
- To ensure adults, including parents, are clear about procedures for misuse of any technologies both within and beyond the school or educational setting.
- To develop links with parents/carers and the wider community ensuring input into policies and procedures.

4. Responsibilities of the school

4.1 Headteacher and Governors

The Headteacher and Governors have overall responsibility for Online Safety as part of the wider remit of safeguarding and child protection. To meet these responsibilities, the following measures are in place:

- The Headteacher has designated an Online Safety Lead to implement agreed policies, procedures, staff training, curriculum requirements and take the lead responsibility for ensuring e-Safety is addressed appropriately. All staff and pupils are aware of who holds this post within the school.
- Time and resources are provided for the e-Safety Lead and staff to be trained and update policies, where appropriate.
- The Headteacher promotes Online Safety across the curriculum and has an awareness of how this is being developed, linked with the school development plan.
- The Headteacher will inform the Governors about the progress of or any updates to the Online Safety curriculum (via PSHE or Computing) and ensure they know how this relates to child protection.
- The Governors (MUST) ensure that Online Safety is embedded within all Child Protection training, guidance and practices.
- An Online Safety Governor has been elected to challenge the school about:
  o Firewalls
  o Anti-virus and anti-spyware software
  o Filters
  o Using an accredited ISP (internet Service Provider)
  o Awareness of wireless technology issues
  o Clear policies on using personal devices.
  o Procedures for misuse, allegations or dealing with Online Safety incidents.

4.2 Online Safety Lead

It is the role of the designated Online Safety Lead to:

- Recognise the importance of Online Safety and understand the school's duty of care to ensure the safety of their pupils and staff.
- Establish and maintain a safe ICT learning environment within the school.
- Update the AUP annually and share it with staff and parents where appropriate.
- Ensure that filtering is set to the correct level for staff, pupils and young people accessing school equipment, or ensure that the technician is informed and carries out work as directed.
- Ensure that all adults understand how filtering levels operate and their purpose.
- Report issues and update the Headteacher on a regular basis.
- Liaise with the PSHE, Safeguarding and Computing leads so that policies and procedures are updated and take into account any emerging issues and technologies.
- Co-ordinate or deliver staff training according to new and emerging technologies so that the correct online safety information can be taught or adhered to.
- Make staff aware of the LSCBN Safeguarding Procedures at www.proceduresonline.com/northamptonshire/scb/

- Implement a system of monitoring staff and pupil use of school issued technologies and the internet, where appropriate. This will be done by monitoring issues when concerns are raised.
- Maintain an Online Safety Incident Log, to be shared with the Headteacher and Governors at agreed intervals.
- Train staff on how to log an Online Safety incident.
- Ensure that anti-virus software and anti-spyware is updated on the network, PCs and teacher/child laptops and that this is reviewed on a regular basis.
- Oversee monitoring of internal emails, where:
  - Blanket e-mails are discouraged
  - Tone of e-mails is in keeping with all other methods of communication
- Look at and monitor how Online-Safety is taught throughout KS2 to ensure coverage in line with the government and OFSTED guidance.

4.3 Staff

It is the responsibility of all adults within the school to:

- Know who the Designated Lead for Safeguarding is, so that any misuse or incidents involving a child can be reported. Please refer to section on Managing Allegations Against Staff for further details.
- Be familiar with, or know where to access school policies, including Safeguarding, Anti-bullying, Disciplinary Procedures and Codes of Conduct.
- Check the filtering levels are appropriate for their pupils and are set at the correct level. Report any concerns to the Online Safety Lead.
- Be aware of new and upcoming programmes, such as Whatsapp and Snapchat, that pupils are using and be aware of the age limit/ risks associated with them. Attend training for updates on changes to the curriculum and the requirements of teachers.
- Ensure that children and young people are protected and supported in their use of technologies so that they know how to use them in a safe and responsible manner. Children and young people should know what to do in the event of an Online Safety incident.
- Communicate with current or past pupils, and their parents/carers, via school authorised channels only (i.e. using professional email addresses and telephone numbers.) All communications with young people should be for school purposes only, unless otherwise authorised by the Headteacher, to minimise the risk of allegations being made against staff.
- Personal communications (such as social networking links) with young people currently in their care are strictly prohibited.
- Understand that behaviour in their personal lives may impact upon their work with children and young people if/when shared online or via social networking sites.
- Ensure that if a social networking site is used, details are not shared with children and young people and privacy settings are set to a maximum.
- Keep usernames and passwords private and never leave work stations unattended when logged in.
- Report accidental access to inappropriate materials to the Online Safety Leader to allow for sites to be added to the restricted list.
- Be mindful of transportation of sensitive pupil/colleague information and photographs on memory sticks, laptops or other devices between school and home.

Wherever possible, encryption or password protection should be used to restrict unauthorised access in the event of loss or theft.

- Address online safety incidents regularly throughout the year and ensure that sessions are planned into the curriculum to remind pupils of the importance of staying safe online. Plan in opportunities for pupils put their knowledge of online safety into practice.

4.4 Children and young people

Children and young people are responsible for:

- Signing agreement to, and abiding by, the Acceptable Use Rules set.
- Using the internet and technologies in a safe and responsible manner within school and at home.
- Informing staff of any inappropriate materials or contact from strangers immediately, without reprimand (age and activity dependent).
- Actively participating in the development and annual review of the Acceptable Use Rules.

5. Appropriate and Inappropriate Use

5.1 By staff or adults

To ensure that both young people and staff are appropriately safeguarded against online risks and allegations, a copy of the Acceptable Use Policy will be made accessible to all. The policy clearly highlights any behaviours or practices, linked to staff use of technologies, which are deemed inappropriate by HM Government 'Safer Working Practice' guidelines or other relevant safeguarding legislation and professional standards. Staff are expected to take responsibility for their own use of technology and are asked to read and sign acceptance of the staff acceptable use rules annually (see Appendix 1 for template).

Examples of inappropriate use:

- Accepting or requesting current or past pupils as 'friends' on social networking sites, or exchanging personal email addresses or mobile phone numbers.
- Behaving in a manner which would lead any reasonable person to question a staff member's suitability to work with pupils or act as a role model. This would include inappropriate comments, photographs or videos on social networking sites which reflect badly on either the individual, their colleagues or the school/workplace.

In the event of inappropriate use:

If a member of staff is believed to misuse the internet in an illegal, inappropriate or abusive manner, a report must be made to the Headteacher/Safeguarding Lead immediately. If the allegation of inappropriate use is aimed at the Head Teacher then the report will be made to the Chair of the Governing Body. The appropriate NSCB allegation procedures and child protection policies must be followed to deal with any misconduct and all relevant authorities contacted.
In the lesser event of minor or accidental misuse, internal staff disciplinary procedures will be referred to in terms of any action to be taken.

5.2 By Children or Young People

The student Acceptable Use Rules provide children and young people with clear guidelines on appropriate use of the internet and technologies within school and are linked to school disciplinary procedures. Pupils sign acceptance of the rules when they join the school and they are displayed throughout the school as a reminder.

To encourage parental/carer support of the student Acceptable Use Rules, a copy is sent home with the related school sanctions for misuse. This is also displayed on the school website and is clearly seen around school.
Parents/carers are asked to sign the Acceptable Use Rules with their child annually to show their support of the online safeguarding rules in place.

In the event of inappropriate use

If a child or young person is found to misuse online technologies or equipment whilst at school, the following sanctions will apply:

- Failure to abide by Acceptable Use Rules and deliberate misuse of the internet/technologies will result in a letter being sent home to parents/carers explaining the reason for suspending the child or young person's use for a particular lesson or activity.
- Further misuse of the rules may result in withdrawal of a student's internet privileges for a period of time and another letter sent home to parents/carers.
- A letter may be sent to parents/carers outlining the breach in the Safeguarding Policy where a child or young person is deemed to have misused technology against another child or adult.

In the event of accidental access to inappropriate materials, pupils are expected to notify an adult immediately and attempt to minimise or close the content until an adult can take action. In the event of a member of staff being aware of a child having a Facebook/ Twitter account, a letter will be sent home to their parents informing them of this and reminding them of the legal age requirement. Appropriate Online Safety incident procedures are then followed.

6. The Curriculum

6.1 Internet use

It is the responsibility of schools to teach their pupils how to use the internet safely and responsibly. The following concepts, skills and competencies will be developed through both the PSHE and ICT curriculum:

- Internet literacy
- making good judgements about websites and emails received
- knowledge of risks such as viruses and opening mail from a stranger
- knowledge of copyright and plagiarism issues
- file-sharing and downloading illegal content
- uploading personal information – what is and is not safe
- where to go for advice and how to report abuse.

It is also the schools' responsibility to plan in opportunities for pupils to make informed judgements and manage risks themselves rather than relying on filtering systems.

Online personal safety is taken extremely seriously within our school community and our pupils are encouraged to refrain from sharing personal information in any form of electronic communications. Personal informal includes:

- full name
- address
- telephone number
- email address

6.2 Pupils with additional learning needs

The school strives to provide access to a broad and balanced curriculum for all learners and recognises the importance of tailoring activities to suit the educational needs of each pupil. Where a student has specific learning requirements, or poor social understanding, careful consideration is given to the planning and delivery of online safety awareness sessions and internet access.

6.3 Email use

Pupils

Pupils are introduced to, and use email as part of the Computing Curriculum. They are provided with email accounts to use, as part of their entitlement to understand different ways of communicating and using ICT to share and present information. Pupils will use this email account for any form of school related communications (i.e. homework) and teaching staff will regularly monitor their class use of these systems. Teachers may want to pass this on to parents as a form of communication. Children's emails are set as their first name and second name followed by iflt.org.uk. If there are any cases where a child (for safeguarding purposes) cannot use this set up, alternative options should be offered, such as the email being turned off or directed to the class teacher. Pupils should be encouraged to keep and update their password. They will be taught the importance of password protections. They should not use this email to sign up for any other sites.

Staff

Professional email addresses will be used for all electronic correspondence between staff and pupils, and for school related business only. This is true also for any communications with parents or carers. Under no circumstances will staff members engage in personal communications (i.e. via hotmail or yahoo accounts) with current or former pupils outside of authorised school systems. The use of professional email accounts allows for content monitoring to take place and minimises the risk of allegations being made against staff. Passwords should be kept and never shared with any third party for email accounts or computer login access.

6.4 Mobile technologies

Everyday technologies, including mobile phones, mp3 players, tablets and handheld games consoles, are increasingly being used by both adults and children within the school environment. For this reason, appropriate safeguards must be in place to protect young people and staff against the following associated risks:

- Inappropriate or bullying text messages
- Images or video taken of adults or peers without permission
- Videoing violent, unpleasant or abusive acts towards a peer or adult which may be distributed
- Sexting- the sending of suggestive or sexually explicit personal images via mobile phones
- Wireless internet access which can bypass school filtering and allow access to inappropriate or potentially harmful material or communications.

All teachers have their own iPads to use when taking photos. No personal devices or mobile phones should be used for this. Devices are regularly monitored and wiped clear throughout the academic year.

6.4.1 Mobile phones

Pupil Use:

Pupils are advised NOT to bring mobile phones to school. If there is an agreement by a member of SLT and a parent because of a 'special circumstance,' they are kept in the office safe for safekeeping. If there is reason to suspect that a student's mobile device contains inappropriate, illegal or harmful content, whilst on school grounds, it will be confiscated by staff and may be searched. The Online Safety Incident and Child Protection procedures will be followed if such content is discovered.

Staff Use:

Staff may bring personal mobile phones into school, but they will be used outside of lesson time only. Under no circumstances will staff use their personal mobile phone to communicate with current or former pupils or their parents/carers. School telephone numbers will be used for this purpose, apart from when on off-site school trips. If there is an urgent situation where an adult needs to communicate with a parent whilst they are off-site, then they must withhold their number before calling. All images or video recordings of children and young people will be taken using school equipment, never personal camera phones or other such devices. It is the responsibility of staff to ensure that no inappropriate or illegal content is stored on their device when bringing it onto school grounds.

6.4.2 Laptops/Tablets

Teaching staff are provided with school laptops and an iPad to allow for school related work to be completed off site. These are encrypted and password protected and should not be used by family members. Memory sticks for transferring information between school and home should not be used unless purchased by the school and have appropriate encryption software activated.

6.5 Video and photographs

Images or videos featuring pupils will only feature on the school website or in press coverage if permission has been granted by parents/carers in advance. Wherever possible group shots of children will be taken, as opposed to images of an individual and first names only will be displayed. Photographs should not show children in compromising positions or in inappropriate clothing (e.g. gym kit, swimming costumes). Only school equipment will be used to take any images of pupils.

6.6 Video-conferencing and webcams

To safeguard staff and young users, publicly accessible webcams are not to be used in school. As with video and photographs, permission will be sought from parents/carers before a child engages in video conferencing with individuals or groups outside of the school setting (e.g. communicating with a school overseas) All video conferencing will be supervised by staff and a record of dates, times and participants held in school for audit trail purposes.

7. Web 2.0 Technologies

7.1 Managing Social Networking and other Web 2.0 technologies

Social networking is now the communication form of choice for many adults and young people worldwide and, as a result, safeguards must be in place to ensure that staff and pupils are aware of the risks associated with this form of technology. To address this issue, a series of preventative measures are in place:

- The first 3 weeks of September will be dedicated to teaching the children about how to stay safe online. This will be referred to in all future lessons where the internet is used.
- Access to social networking sites is controlled through the school internet filtering systems.
- Pupils and staff are discouraged from providing personal details or identifiable information on profiles (e.g. mobile number, address, school name, clubs attended, email address or full names of friends). Children are asked to include images of avatars for their display icon instead of real pictures.
- Pupils and staff are made aware of the risks of posting images online and how publicly accessible their content is. Background images in photographs which may reveal personal details are also addressed (e.g. house number, street name, school uniform)
- Social networking security settings are explained and recommendations made for privacy settings to be activated to 'Friends only' for all applications to restrict unsolicited access. The importance of passwords and blocking of unwanted communications is also highlighted.
- Comments on the blogs are regularly monitored, with the teacher modelling appropriate responses which should be left.
- Both online and school systems for reporting abuse or unpleasant content, i.e. cyberbullying, are reinforced www.thinkuknow.co.uk.

7.2 Staff using social networks

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, staff have a responsibility to ensure that their actions outside of school do not impact on their work with children and young people. HM Gov 'Safer Working Practice' clearly states that adults working with children should:

- Only make contact with pupils for professional reasons and with the authorisation of the Headteacher. Any communication should be via professional email only and never through a personal email account.

- Ensure that if a social networking account is used, details are not shared with children and young people and privacy settings are set to a maximum.
- Be aware that behaviour in their personal lives may impact on their work with children and young people.
- Not behave in a manner which would lead any reasonable person to question their suitability to work with children and young people.

8. Safeguarding measures

8.1 Filtering

Surf Protect filtering system provides a filtered internet service to Finedon Schools, which prevents access to illegal and inappropriate sites. The school has access to a local control list which allows websites to be added to a 'restricted list'.

Changes to the filtering will be agreed by the Headteacher and Online Safety Officer, these changes will be implemented the Computing Subject Lead / Online Safety Officer.

In addition to the above, the following safeguards are also in place:

- Reports can be produced from the school's filtering system, SurfProtect, which show what websites and search queries have been blocked.
- Anti-virus and anti-spyware software is used on all network and stand-alone PCs or laptops and is updated on a regular basis.
- A firewall ensures information about children and young people and the school cannot be accessed by unauthorised users.
- Links to online safety websites are provided on the school website.
- Encryption codes on wireless systems prevent hacking.

8.2 Tools for bypassing filtering

Web proxies are the most popular and successful method for pupils to bypass internet filters in order to access unauthorised online content on the school network. A web proxy is capable of hiding the IP address of the user and opening unrestricted and, in cases, unidentifiable channels through which blocked material can be viewed e.g. Social networking sites, gaming websites or adult content.
To manage this safeguarding concern, pupils and staff are forbidden to use any technology designed to circumvent, avoid or bypass school security controls (including internet filters, antivirus solutions or firewalls). Violation of this rule by either staff or pupils will result in school sanctions being applied.

9. Parents

9.1 Roles

Each student will receive a copy of the Acceptable Use Rules on an annual basis or first-time entry to the school. Pupils and their parents/carers are asked to read and sign acceptance of the student Acceptable Use Rules to be returned to, and stored by, the school.

9.2 Support

As part of the school's approach to developing online safety awareness with children and young people, every effort is made to offer parents/carers the opportunity to find out more about how they can support their child to stay safe online within and beyond the school environment. Online Safety Parent/Carer Information Sessions will be held annually to raise awareness of key internet safety issues and highlight safeguards currently in place at school (e.g. filtering and training in place to minimise online risk.) Free to order resources from Childnet (http://www.childnet-int.org/kia/parents/) and the Thinkuknow website (http://www.thinkuknow.co.uk/teachers/resources/) can be used to support this. Wherever possible, the school will endeavour to provide internet access for parents/carers without this resource at home, to ensure that appropriate advice and information on this topic can be viewed.

10. Links to other policies

10.1 Behaviour, Cyberbullying and Anti-Bullying
The Acceptable Use Policy is cross-referenced throughout a number of other policies in place throughout the school, including those for behaviour, anti-bullying, PSHE and child protection. Cyberbullying features within the school's anti-bullying policy due to the growing number of incidents recorded. Cyberbullying will not be tolerated in or outside of school and clear procedures for dealing with cyberbullying incidents can be found within the anti-bullying policy.

10.2 Managing allegations and concerns of abuse made against people who work with children.

The LSCBN Allegations Procedure www.proceduresonline.com/northamptonshire/scb/ will be referred to in the event that an allegation of misuse or misconduct is made by a child or other adult about a member of staff.
Allegations made against staff members must be reported to the Designated Person for Child Protection within school immediately. In the event of an allegation being made against the Headteacher, the Chair of Governors will be notified immediately.

10.3 PSHE

The teaching and learning of Online Safety is embedded within the PSHE curriculum to ensure that the key safety messages about engaging with people are the same whether children and young people are on or offline.

10.4 School website

Permission will be sought from parents/carers prior to the uploading of any images onto the school website. Consideration is given to which information is relevant to share with the general public on a website and secure areas will be used for information pertaining to specific audiences. The schools AUP will also be published on this platform along with recommended websites.

10.5 Disciplinary Procedure for All School Based Staff

In the event that a staff member is seen to be in breach of professional standards of conduct or is believed to have misused online technologies, school disciplinary procedures and sanctions will be applied.

Signed……..

Chair of Governors

Date ……..

Written in September 2017

Next Review September 2018