THE FLITCH GREEN
ACADEMY
Learning for life

E-Safety Policy

Created 01/05/2014
Ratified by FGB on 08/12/2016
To be reviewed December 2019
Audit and Risk Committee to Oversee

The Flitch Green Academy recognises that ICT and the internet are fantastic tools for learning and communication that can be used in school to enhance the curriculum, challenge pupils, and support creativity and independence. Using ICT to interact socially and share ideas can benefit everyone in the school community, but it is important that the use of the internet and ICT is seen as a responsibility and that pupils, staff and parents use it appropriately and practice good e-safety. It is important that all members of the school community are aware of the dangers of using the internet and how they should conduct themselves online.

E-safety covers the internet but it also covers mobile phones and other electronic communications technologies. We know that some adults and young people could use these technologies to harm children. The harm might range from sending hurtful or abusive texts and emails, to enticing children to engage in sexually harmful conversations or actions online, webcam filming, photography or face-to-face meetings. There is a 'duty of care' for any persons working with children and educating all members of the school community on the risks and responsibilities of e-safety falls under this duty. It is important that there is a balance between controlling access to the internet and technology and allowing freedom to explore and use these tools to their full potential. This policy aims to be an aid in regulating ICT activity in school, and provide a good understanding of appropriate ICT use that members of the school community can use as a reference for their conduct online outside of school hours. E-safety is a whole-school issue and responsibility.

Cyber-bullying by pupils will be treated as seriously as any other type of bullying and will be managed through our anti-bullying procedures.

1. **Roles and responsibility**

The school e-Safety Coordinator is Nathan Lowe. The designated member of the Governing Body responsible for e-safety is Nikki Brazier.

2. **Communicating school policy**

This policy is available on the school website for parents, staff, and pupils to access when and as they wish. E-safety is integrated into the curriculum in any circumstance where the internet or technology are being used, and during PSHE lessons where personal safety, responsibility, and development are being discussed.

3. **Making use of ICT and the internet in school**

The internet is used in school to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions. Technology is advancing rapidly and is now a huge part of everyday life, education and business. We want to equip our students with all the necessary ICT skills that they will need in order to enable them to progress confidently into a professional working environment when they leave school.

Some of the benefits of using ICT and the internet in schools are:

For pupils:

- Unlimited access to worldwide educational resources and institutions such as art galleries, museums and libraries.
- Contact with schools in other countries resulting in cultural exchanges between pupils all over the world.
- Access to subject experts, role models, inspirational people and organisations. The internet can provide a great opportunity for pupils to interact with people that they otherwise would never be able to meet.
- An enhanced curriculum; interactive learning tools; collaboration, locally, nationally, and globally; self-evaluation; feedback and assessment; updates on current affairs as they happen.
- Access to learning whenever and wherever convenient.
- Freedom to be creative.
- Freedom to explore the world and its cultures from within a classroom.
- Social inclusion, in class and online.
- Access to case studies, videos and interactive media to enhance understanding.
- Individualised access to learning.

For staff:

- Professional development through access to national developments, educational materials and examples of effective curriculum practice and classroom strategies.
- Immediate professional and personal support through networks and associations.
- Improved access to technical support.
- Ability to provide immediate feedback to students and parents.
- Class management, attendance records, schedule, and assignment tracking.

4. Learning to evaluate internet content

With so much information available online it is important that pupils learn how to evaluate internet content for accuracy and intent. This is approached by the school as part of digital literacy across all subjects in the curriculum. Students will be taught:

- to be critically aware of materials they read, and shown how to validate information before accepting it as accurate
- to use age-appropriate tools to search for information online
- to acknowledge the source of information used and to respect copyright.

The school will also take steps to filter internet content to ensure that it is appropriate to the age and maturity of pupils. If staff or pupils discover unsuitable sites then the URL will be reported to the *school e-safety coordinator.* Any material found by members of the school community that is believed to be unlawful will be reported to the appropriate agencies. Regular software and broadband checks will take place to ensure that filtering services are working effectively.

5. Managing information systems

The school is responsible for reviewing and managing the security of the computers and internet networks as a whole and takes the protection of school data and personal protection of our school community very seriously. This means protecting the school network, as far as is practicably possible, against viruses, hackers and other external security threats. The security of the school information systems and users will be reviewed regularly by and virus protection software will be updated regularly.

6. Emails

The school uses email internally for staff and externally for contacting parents and other stakeholders, and is an essential part of school communication.

Staff should be aware that school email accounts should only be used for school-related matters, i.e. for staff to contact parents, other members of staff and other professionals for work purposes. This is important for confidentiality. The school has the right to monitor emails and their contents but will only do so if it feels there is reason to.

6.2 School email accounts and appropriate use

Staff should be aware of the following when using email in school:

- Staff should only use official school-provided email accounts to communicate with pupils, parents or carers. Personal email accounts should not be used to contact any of these people and should not be accessed during school hours.
- Emails sent from school accounts should be professionally and carefully written. Staff are representing the school at all times and should take this into account when entering into any email communications.
- Staff must tell their line manager or a member of the senior leadership team if they receive any offensive, threatening or unsuitable emails either from within the school or from an external account. They should not attempt to deal with this themselves.
- The forwarding of chain messages is not permitted in school.

Pupils should be aware of the following when using email in school, and will be taught to follow these guidelines through the ICT curriculum and in any instance where email is being used within the curriculum or in class:

- in school, pupils should only use school-approved email accounts
- excessive social emailing will be restricted
- pupils should tell a member of staff if they receive any offensive, threatening or unsuitable emails either from within the school or from an external account. They should not attempt to deal with this themselves.
- pupils must be careful not to reveal any personal information over email, or arrange to meet up with anyone who they have met online without specific permission from an adult in charge.

Pupils will be educated to identify spam, phishing and virus emails and attachments that could cause harm to the school network or their personal account or wellbeing.

7. Published content and the school website

The school website is viewed as a useful tool for communicating our school ethos and practice to the wider community. It is also a valuable resource for parents, students, and staff for keeping up-to-date with school news and events, celebrating whole-school achievements and personal achievements, and promoting school projects.

The website is in the public domain, and can be viewed by anybody online. Any information published on the website will be carefully considered in terms of safety for the school community, copyrights and privacy policies. No personal information on staff or pupils will be published, and details for contacting the school will be for the school office only. **For information on the school policy on children's photographs on the school website please refer to section 7.2 of this policy.**

7.2 Policy and guidance of safe use of children's photographs and work

Colour photographs and pupils work bring our school to life, showcase our pupil's talents, and add interest to publications both online and in print that represent the school. However, the school acknowledges the importance of having safety precautions in place to prevent the misuse of such material.

Under the Data Protection Act 1998 images of pupils and staff will not be displayed in public, either in print or online, without consent. On admission to the school parents/carers will be asked to sign a photography consent form. The school does this so as to prevent repeatedly asking parents for consent over the school year, which is time-consuming for both parents and the school. The terms

of use of photographs never change, and so consenting to the use of photographs of your child over a period of time rather than a one-off incident does not affect what you are consenting to.

Using photographs of individual children

The vast majority of people who take or view photographs or videos of children do so for entirely innocent, understandable and acceptable reasons. Sadly, some people abuse children through taking or using images, so we must ensure that we have some safeguards in place.

It is important that published images do not identify students or put them at risk of being identified. Only images created by or for the school will be used in public and children may not be approached or photographed while in school or doing school activities without the school's permission. The school follows general rules on the use of photographs of individual children:

- Parental consent must be obtained. Consent will cover the use of images in:
  - all school publications
  - on the school website
  - in newspapers as allowed by the school
  - in videos made by the school or in class for school projects.
- Electronic and paper images will be stored securely.
- Names of stored photographic files will not identify the child.
- Images will be carefully chosen to ensure that they do not pose a risk of misuse. This includes ensuring that pupils are appropriately dressed. Photographs of activities which may pose a greater risk of potential misuse (for example, swimming activities), will focus more on the sport than the pupils (i.e. a pupil in a swimming pool, rather than standing by the side in a swimsuit).
- For public documents, including in newspapers, full names will not be published alongside images of the child. Groups may be referred to collectively by year group or form name.
- Events recorded by family members of the pupils such as school plays or sports days must be used for personal use only.
- Pupils are encouraged to tell a member staff if they are concerned or uncomfortable with any photographs that are taken of them or they are being asked to participate in.
- Any photographers that are commissioned by the school will be fully briefed on appropriateness in terms of content and behaviour, will wear identification at all times, and will not have unsupervised access to the pupils. For more information on safeguarding in school please refer to our **Child Protection Policy.**

6.3 Complaints of misuse of photographs or video

Parents should follow standard school complaints procedure if they have a concern or complaint regarding the misuse of school photographs. Please refer to our **Complaints Policy** for more information on the steps to take when making a complaint. Any issues or sanctions will be dealt with in line with the schools **Child Protection Policy** and **Behaviour policy.**

6.4 Social networking, social media and personal publishing

Social media sites have many benefits for both personal use and professional learning; however, both staff and pupils should be aware of how they present themselves online. Pupils are taught through the ICT curriculum and PSHE about the risks and responsibility of uploading personal information and the difficulty of taking it down completely once it is out in such a public place. The school follows general rules on the use of social media and social networking sites in school:

- Pupils are educated on the dangers of social networking sites and how to use them in safe and productive ways. They are all made fully aware of the school's code of conduct regarding the use of ICT and technologies and behaviour online.
- Any sites that are to be used in class will be risk-assessed by the teacher in charge prior to the lesson to ensure that the site is age-appropriate and safe for use.
- Official school blogs created by staff or pupils/year groups/school clubs as part of the school curriculum will be controlled by a member of staff and will be moderated by a member of staff.
- Pupils and staff are encouraged not to publish specific and detailed private thoughts, especially those that might be considered hurtful, harmful or defamatory. The school expects all staff and pupils to remember that they are representing the school at all times and must act appropriately.
- Safe and professional behaviour of staff online will be discussed at staff induction.

8. Mobile phones and personal device

Staff

- Under no circumstances should staff use their own personal devices to contact pupils either in or out of school time.
- Staff are not permitted to take photos or videos of pupils. If photos or videos are being taken as part of the school curriculum or for a professional capacity, the school equipment will be used for this.
- The school expects staff to lead by example. Personal mobile phones should be switched off or on 'silent' during school hours.

- Any breach of school policy may result in disciplinary action against that member of staff. More information on this can be found in the **Child Protection Policy**, or in the staff contract of employment.

9. Cyberbullying

Cyberbullying, as with any other form of bullying, is taken very seriously by the school. Information about specific strategies or programmes in place to prevent and tackle bullying are set out in the **Behaviour Policy.** The anonymity that can come with using the internet can sometimes make people feel safe to say and do hurtful things that they otherwise would not do in person. It is made very clear to members of the school community what is expected of them in terms of respecting their peers, members of the public and staff, and any intentional breach of this will result in disciplinary action.

If an allegation of bullying does come up, the school will:

- take it seriously
- act as quickly as possible to establish the facts. It may be necessary to examine school systems and logs or contact the service provider in order to identify the bully
- record and report the incident
- provide support and reassurance to the victim
- make it clear to the 'bully' that this behaviour will not be tolerated. If there is a group of people involved, they will be spoken to individually and as a whole group. It is important that children who have harmed another, either physically or emotionally, redress their actions and the school will make sure that they understand what they have done and the impact of their actions.

If a sanction is used, it will correlate to the seriousness of the incident and the 'bully' will be told why it is being used. They will be asked to remove any harmful or inappropriate content that has been published, and the service provide may be contacted to do this if they refuse or are unable to remove it. They may have their internet access suspended in school.

Repeated bullying may result in a fixed-term exclusion.

10. Managing emerging technologies

Technology is progressing rapidly and new technologies are emerging all the time. The school will risk-assess any new technologies before they are allowed in school, and will consider any educational benefits that they might have. The school keeps up-to-date with new technologies and is prepared to quickly develop appropriate strategies for dealing with new technological developments.

11. Protecting personal data

The Flitch Green Academy believes that protecting the privacy of our staff and pupils and regulating their safety through data management, control and evaluation is vital to whole-school and individual progress. The school collects personal data from pupils, parents, and staff and processes it in order to support teaching and learning, monitor and report on pupil and teacher progress, and strengthen our pastoral provision.

We take responsibility for ensuring that any data that we collect and process is used correctly and only as is necessary, and the school will keep parents fully informed of the how data is collected, what is collected, and how it is used. National curriculum results, attendance and registration records, special educational needs data, and any relevant medical information are examples of the type of data that the school needs. Through effective data management we can monitor a range of school provisions and evaluate the wellbeing and academic progression of our school body to ensure that we are doing all we can to support both staff and students.

In line with the Data Protection Act 1998, and following principles of good practice when processing data, the school will:

- ensure that data is fairly and lawfully processed
- process data only for limited purposes
- ensure that all data processed is adequate, relevant and not excessive
- ensure that data processed is accurate
- not keep data longer than is necessary
- process the data in accordance with the data subject's rights
- ensure that data is secure
- ensure that data is not transferred to other countries without adequate protection.

There may be circumstances where the school is required either by law or in the best interests of our students or staff to pass information onto external authorities; for example, our local authority, Ofsted, or the Department of Health. These authorities are up-to-date with data protection law and have their own policies relating to the protection of any data that they receive or collect.

For more information on the school's safeguards relating to data protection read the school's **Data Protection Policy.**

Appendices

Staff Procedures Following Misuse by Staff

The Principal will ensure that these procedures are followed, in the event of any misuse of the Internet, by an adult:

A. An inappropriate website is accessed inadvertently:
Advise the Principal immediately, who will contact the helpdesk filtering service for the academy so that it can be added to the banned or restricted list.

B. An inappropriate website is accessed deliberately:
Ensure that no one else can access the material by shutting down.
Log the incident.
Principal to refer back to the Acceptable Use Rules and follow agreed actions for discipline.
Inform the helpdesk filtering services as with A.

C. An adult receives inappropriate material.
Do not forward this material to anyone else – doing so could be an illegal activity.
Ensure the device is removed and log the nature of the material.
Contact relevant authorities for further advice e.g. police.

D. An adult has used IT equipment inappropriately:
Follow the procedures for B.

E. An adult has communicated with a child or used IT equipment inappropriately:
Report Immediately to the Principal
Ensure the child is reassured and remove them from the situation immediately, if necessary.
Report to the Designated Person for Child Protection (Principal) immediately, who should then follow the Allegations Procedure and Child Protection Policy
Preserve the information received by the child if possible and determine whether the information received is abusive, threatening or innocent.
Once Procedures and Policy have been followed and the incident is considered innocent, refer to the Acceptable Use Rules for Staff and Principal to implement appropriate sanctions.
If illegal or inappropriate misuse is known, contact the Principal or Chair of Governors (if allegation is made against the Principal) and

Designated Person for Child Protection immediately and follow the Allegations procedure and Child Protection Policy.
Contact the Police/Social Services as necessary.

F. Threatening or malicious comments are posted to the academy
Preserve any evidence.
Inform the Principal immediately and follow Child Protection Policy as necessary.
Contact the Police/Social Services as necessary.

G. Where staff or adults are posted on inappropriate websites or have inappropriate information about them posted this should be reported to the Principal.

Staff Procedures Following Misuse by Children

The Principal will ensure that these procedures are followed, in the event of any misuse of the Internet by a child:

A. An inappropriate website is accessed inadvertently:
Reassure the child that they are not to blame and praise for being safe and responsible by telling an adult.
Report website to the Principal if this is deemed necessary.
Contact the helpdesk filtering service so that it can be added to the banned list.
Check the filter level is at the appropriate level for staff use in the academy.

B. An inappropriate website is accessed deliberately:
Refer the child to the Acceptable Use Rules that were agreed.
Reinforce the knowledge that it is illegal to access certain images and police can be informed.
Decide on appropriate sanction.
Notify the parent/carer.
Inform helpdesk as above.

C. An adult or child has communicated with a child or used IT equipment inappropriately:
Ensure the child is reassured and remove them from the situation immediately.
Report to the Principal immediately.
Preserve the information received by the child if possible and determine whether the information received is abusive, threatening or innocent.
If illegal or inappropriate misuse the Principal must follow the Allegation Procedure and/or Child Protection Policy
Contact the Police/Social Services as necessary.

D. Threatening or malicious comments are posted to the academy website about a child in the academy:
Preserve any evidence.
Inform the Principal immediately.
Inform the e-Safety Leader so that new risks can be identified.
Contact the Police/Social Services as necessary.

E. Threatening or malicious comments are posted on external websites about an adult in the academy:
Preserve any evidence.
Inform the Principal immediately.

Acceptable Use Rules for Staff

These rules apply to all on-line use and to anything that may be downloaded or printed.

To ensure that all adults within the academy are aware of their responsibilities when using any technologies, such as the Internet or E-mail, they are asked to sign these Acceptable Use Rules. This is so that they provide an example to children for the safe and responsible use of on-line technologies, which will educate, inform and protect and so that they feel safeguarded from any potential allegations or inadvertent misuse themselves.

- I know that I should only use the academy equipment in an appropriate manner and for professional uses.
- I understand that I need to give permission to children before they can upload images (film or photographs) to the Internet or send them via E-mail.
- I know that images should not be inappropriate or reveal any personal information of children if uploading to the Internet.
- I have read the Procedures for Incidents of Misuse so that I can deal with any problems that may arise, effectively.
- I will report accidental misuse.
- I will report any incidents of concern for children's safety to the Principal (Designated Person for Child Protection and e-Safety Leader) in accordance with procedures listed in the Acceptable Use Policy.
- I know who my Designated Person for Child Protection is.
- I know that I am putting myself at risk of misinterpretation and allegation should I contact children via personal technologies, including my personal e-mail and should use the academy E-mail and phones (if provided) and only to a child's school E-mail address upon agreed use within the academy.
- I know that I should not be using the academy system for personal use unless this has been agreed by the Principal.
- I know that I should complete virus checks on my laptop and memory stick or other devices so that I do not inadvertently transfer viruses, especially where I have downloaded resources.
- I will only install hardware and software I have been given permission for.
- I will ensure messages are written carefully and politely, particularly as an e-mail could be forwarded to unintended readers.
- I will ensure that I keep my password secure and not disclose any security information unless to appropriate personnel. If I feel someone inappropriate requests my password I will check with the Principal.
- I have been given a copy of the Acceptable Use Policy to refer to about all e-safety issues and procedures that I should follow.
- I will adhere to copyright and intellectual property rights.

I have read, understood and agree with these Rules as I know that by following them I have a better understanding of e-Safety and my responsibilities to safeguard children when using on-line technologies.

Signed……..Date…….

Name (printed)…….

School…The Flitch Green Academy ……..

Letter to Parents of The Flitch Green Academy

Dear Parent/Carer,

As part of an enriched curriculum your child will be accessing the Internet and e-mail via Essex County Council's broadband system.

In order to support the academy in educating your child about e-Safety (safe use of the Internet), please read the following Rules with your child then sign and return the slip to the academy office.

In the event of a breach of the Rules by any child, the e-Safety Policy lists further actions and consequences, should you wish to view it.

These Rules provide an opportunity for further conversations between you and your child about safe and appropriate use of the Internet and other on-line tools (e.g. mobile phone), both within and beyond the academy (e.g. at a friend's house or at home).

Should you wish to discuss the matter further please contact the Principal.

Yours faithfully,

Chair of the Governing Body

e-Safety Acceptable Use Rules Return Slip
2014 and onwards

Child Agreement:

Name:_____Class:_____

- I understand the Rules for using the Internet, E-mail and on-line tools, safely and responsibly.
- I know that the adults working with me at the academy will help me to stay safe and check that I am using the computers to help me with my work.

Child Signature: _____ Date: _____

Parent/Carer Agreement:

- I have read and discussed the Rules with my child and confirm that he/she has understood what the Rules mean. I give permission for my son/daughter to access the Internet.
- I understand that the academy will take all reasonable precautions to ensure that pupils cannot access inappropriate materials but I appreciate that this is a difficult task. I agree that the academy is not liable for any damages arising from use of the Internet facilities. I understand that occasionally, inappropriate materials may be accessed and accept that the academy will endeavour to deal with any incident that may arise, according to policy.
- I understand that whilst my child is using the Internet and other on-line tools outside of the academy, that it is my responsibility to ensure safe and responsible use with the support of the academy.
- I agree that my son/daughter's work may be electronically published. I also agree that appropriate images and film clips that include my son/daughter may be published subject to the academy rule that photographs will not be accompanied by pupil names

Parent/Carer Signature: _____ Date: _____

Key Stage 1

These are our rules for using the Internet safely.

Our Internet and E-mail Rules

- We use the Internet safely to help us learn.
- We learn how to use the Internet.
- We can send and open messages with an adult.
- We can write polite and friendly e-mails or messages to people that we know.
- We only tell people our first name, or we use a 'made-up' name.
- We learn to keep our password a secret.
- We know who to ask for help.
- If we see something we do not like we know what to do.
- We know that it is important to follow the rules.
- We are able to look after each other by using our safe Internet.
- We can go to www.thinkuknow.co.uk for help.

Key Stage 2

These are our rules for using the Internet safely and responsibly.

Our On-line Rules

- We use the Internet to help us learn and we will learn how to use the Internet safely and responsibly.
- We send e-mails and messages that are polite and friendly.
- We will only e-mail, chat to or video-conference people an adult has approved.
- Adults are aware when we use on-line tools, such as video-conferencing.
- We never give out passwords or personal information (like our surname, address or phone number).
- We never post photographs or video clips without permission and never include names with photographs.
- If we need help we know who to ask.
- If we see anything on the Internet or in an e-mail that makes us uncomfortable, we know what to do.
- If we receive a message sent by someone we don't know we know what to do.
- We know we should follow the rules as part of the agreement with our parent/carer.
- We are able to look after each other by using our safe Internet in a responsible way.
- We know that we can go to www.thinkuknow.co.uk for help.

Further Information and Guidance

:

- www.parentscentre.gov.uk (for parents/carers)
- www.ceop.co.uk (for parents/carers and adults)
- www.iwf.org.uk (for reporting of illegal images or content)
- www.thinkuknow.co.uk (for all children and young people with a section for parents/carers and adults – this also links with the CEOP (Child Exploitation and On-line Protection Centre work)
- www.netsmartzkids.org (5 – 17)
- www.kidsmart.org.uk – (all under 11)
- www.phonebrain.org.uk (for Yr 5 – 8)
- www.bbc.co.uk/cbbc/help/safesurfing (for Yr 3/4)
- www.hectorsworld.com (for FS, Yr 1 and 2 and is part of the thinkuknow website above)
- www.teachernet.gov.uk (for schools and settings)
- www.dcsf.gov.uk (for adults)
- www.digizen.org.uk (for materials from DCSF around the issue of cyberbullying)
- www.becta.org.uk (advice for settings to update policies) and http://www.nextgenerationlearning.org.uk/esafetyandwifi.html (simple tips for parents/adults)
- www.nen.org.uk (for schools and settings – access to the National Education Network)