E Safety and Acceptable Use Policy

'Building for Successful Futures'

Formally adopted by the Governing Board of	Fred Nicholson School
Chair of Governors	Hilary Bradshaw
Policy Holder	Headteacher
Policy Contributor	Heads/Leads of Areas
Last updated	Autumn 2020
To be Reviewed	Autumn 2021 (S&D Committee)

E Safety and Acceptable Use Policy

'Building for Successful Futures'

Introduction

"The Internet and related technologies are powerful tools, which open up new prospects for communication and collaboration. Education is embracing these new technologies as they bring with them fresh opportunities for both teachers and learners.

To use these technologies effectively requires an awareness of the benefits and risks, the development of new skills, and an understanding of their appropriate and effective use both in and outside of the classroom." DfES, eStrategy 2005

The Children Act 2004, Working Together to Safeguard Children (2013) and Keeping Children Safe in Education (2014) sets out how organisations and individuals should work together to safeguard and promote the welfare of children.

This policy aims to:

- Explain the rules and expectations for safe and responsible use of information technology.
- Set out the schools responsibilities for training providing information for pupils, parents and staff in relation the safe responsible use of information technology.
- This Policy document is drawn up to protect all parties – the students, the staff and the school and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements.
- To create a safe working environment for all members of the school community.
- For staff and pupils to be aware of the possible risks online.
- For staff and pupils to know what to do in the event of an e-safety issue

This policy is a constituent of and enhancement to the school's computing policy. It will be reviewed regularly to ensure that it complies with current advice and to include any new developments as appropriate to the schools needs and circumstances.

We use a whole-establishment approach towards responsibility for e-safety:

- Make all staff aware that an E Safety and Acceptable Use Policy and Internet, Social Networking and E Mail Policy is available on the School Directory for them to familiarise themselves with and adhere to.
- Link these policies with other school policies, such as Action Against Bullying. and guidance on copyright and plagiarism.
- Mr M Roach (Deputy Head Teacher) is the designated Senior Management Team member with responsibility for safeguarding and is also the central contact point for all e-safety issues.

- Net Central support Fred Nicholson with the management of their network and the flow of data both in and out of school.
- Headteachers, supported by Governors, should take the lead in embedding the agreed e-safety policies in practice.
- In order to ensure the young people and adults are aware of potential risks and how to practise safe, responsible behaviour, wherever and whenever they are online, the first half-term is set aside in the Scheme of Work for E-Safety learning. However, these issues are also dealt with across the school curriculum, not just at specific times.
- Where there are concerns about the appropriate use of ICT by staff these will be dealt with by the head teacher, through the relevant procedures.

Our e-safety strategy will:

- Allow young people to develop their own protection strategies for when adult supervision and technological protection are not available.
- Give information on where to seek help and how to report incidents.
- Help young people understand that they are not accountable for the actions that others may force upon them but that there are sanctions that the school will impose if they act inappropriately when online;
- Provide guidelines for parents, carers and others on safe practice;
- Ensure we regularly monitor and review our policies with stakeholders;
- Ensure technological solutions are regularly reviewed and updated to ensure maintenance of an effective e-safety programme.

Security and Privacy

- Do not disclose your password to others, do not use passwords intended for others. If you think that others know your password or a pupil's password inform the ICT Manager. Staff should always log out or lock their computer if they leave a workstation unattended. Pupils should not use staff laptops as they are subject to different filtering/ logging protocols.
- Respect and do not attempt to bypass security in place on the computers, or attempt to alter the settings. Report any attempts to do so by pupils to the ICT Manager.
- Ensure that computers are not used in a way that harasses, harms, offends or insults others. Computer filters may be reviewed to ensure that users are using the system responsibly.
- Ensure that pupils do not use computers to cause corruption or destruction to others.
- At no time should staff allow students to access a computer using their own staff account.
- Virus prevention and protection; Fred Nicholson School currently uses Semantic Endpoint Protection.
- Monitoring systems to keep track of who downloaded what, when they downloaded it, using which computer. Fred Nicholson School currently uses Securus Software Limited
- Filtering and content control to minimise inappropriate content via our network. Fred Nicholson School currently uses Netsweeper Incorporated.

- Staff should adhere to the Internet, Social Networking and E Mail use Policy.
- As part of the Local Authorities esafety protocols both the head teacher and deputy head teacher are signed up to the nsix esafety email alerts. Staff and pupils are made aware of this.

Technological devices

Use in School:

- All personal devices must be handed in to the main office at the start of the school day. These will then be collected at the end of the school day
- Virus protection software is installed and updated regularly by the ICT Manager. Staff laptops should be connected to the network at least once a week to allow updates to occur. Pupils should only bring portable storage devices e.g. memory stick, into school with the specific permission from the Headteacher who may liaise with the ICT manager who will check any existing data on these devices for undesirable materials and viruses.
- Pupils should not be allowed to use personal mobile devices during lessons or formal school time unless agreed by the Headteacher.
- Use of the Internet will be monitored and reported on by the ICT Manager as agreed by the Headteacher.

Use in Residential:

- As above
- Pupils are allowed to use personal mobile devices in the care setting when appropriate.
- In the residential setting pupils' usage of the internet is monitored when accessed via the school's network, however, this is not possible if pupils have access to their own internet enabled devices - mobile phones, Ipads/tablets. Parents will be asked to consider the implications of this before allowing them to bring these devices into the residential houses.
- Parents will be advised to monitor their usage and to ensure that privacy settings and filtering software are appropriately applied. School cannot be held accountable for issues that arise from an individual's use of portable devices, but will offer guidance and support to pupils and parents in addressing any issues that arise.
- Parents will be asked to sign a 'Partnership in E safety agreement' before allowing their child to bring a portable internet enabled device into the school or residences.

Misuse of school ICT facilities

If a pupil or member of staff is found to have misused the school systems prompt action will be taken. The E-Safety officers will establish the full facts of the case. He/she will discuss the facts with the Headteacher. Then appropriate action will be taken in line with schools policies and guidance. (The use of a computer system without permission or for a purpose not agreed by the school could constitute a criminal offence under the Computer Misuse Act 1990.)

Use of social networking sites

Rules:
The school recognises that due to the nature of our pupils' complex need and learning difficulties, the rules and consequences regarding their e safety need to be explicit, clear and consistent. Consequences may also need to take into account the individual's intentions and possible social misunderstandings between pupils, according to the given situation.

Rules:

- Pupils must not attempt to make any contact with staff using Facebook, or any other internet site.
- Use their friends' on line accounts to try to contact staff.
- Make false accounts in order to try to contact staff using social networking.
- Upload or write any material which includes a member of staff, taken on the school's site or during school hours.
- Write or upload any material which is offensive or disrespectful to school staff.
- Use Facebook, or any other internet sites, to encourage unkind or inappropriate comments about another pupil, to write derogatory or unkind comments about another pupil, or to use it to arrange or encourage bullying type actions or behaviours.
- Join in with the type of cyber bullying related communication as stated above.
- Set up groups which are inappropriate or offensive about the school.
- Staff will adhere to the Internet, Social Networking and E Mail Use Policy.

Facebook has a page entitled 'Advice for Educators' which may also be of help to staff. CEOP is also a useful organisation for parents and staff to be aware of.

Whilst the school will support staff and pupils as much as is possible, there is a limit to the school's ability to control the pupils access to and usage of the internet and social networking sites out of school hours. The school cannot be held responsible for issues that arise out of school hours, however, if a pupil reports an incident and has evidence such as a print out of the web page, the relevant members of staff will speak to the pupils involved and contact their parents.

The school strongly recommends that parents oversee their child's access to the home computer and internet, as well as other means of using social networking sites such as through Xbox or Play Station, at all times.

For staff:

- All staff have been and will be intermittently reminded that their social networking accounts must have the highest security settings and that

their profile picture, any photographs and any posts must be appropriate.

- Staff have been and will be intermittently reminded not to accept any previous or current pupils as 'friends' on their accounts. It is strongly recommended that staff do not accept any individual with whom they are not familiar. There have been incidents in the news of pupils setting up false accounts in order to gain access to a member of staff's social networking pages.
- This policy will be included in the Induction Information so that all new staff are aware of the expectations regarding social networking.
- Staff should NOT use their own mobile phones for school business unless agreed with the Headteacher.

For parents:

- Training will be available for parents in order to address the issues of cyber bullying and e safety
- A letter will go home to parents at least once a year to remind them to oversee their child's use of the internet in general as well as social networking. They will be reminded that a child should be 13 or over to have their own Facebook account.
- Parents will be contacted directly if there are issues related to their child's use of the internet and online sites they access.
- This policy will be made available to parents via the school's website.
- Primary and secondary pupils receive teaching regarding internet safety and cyber bullying issues as part of their ICT curriculum.
- Pupils and their parents will be encouraged to report any inappropriate use of online facilities to a member of staff. Confidentiality will be respected as far as possible.

References:

- NCC advice on Internet Access Policies
- Superhighway Safety, Children's safe use of the Internet – Becta
- Connecting Schools, Networking People – Becta
- ACITT – Acceptable Use Policy
- eSafety – Becta
- CEOP
- The Child Protection Company

Links to Other Policies
Anti-bullying
Internet, Social Networking & E Mail Use Policy
Computing
Pupil Well Being
Protect Me

Equality Impact Statement
The Governors have reviewed this policy giving due regard to their responsibilities with respect to the equalities agenda, in line with recent legislation. They believe that the policy reflects a positive attitude and approach to all members of the school community.

Policy Approved by:

Chair of Committee 

*To be ratified on 02.12.20