Future Generation Trust

E-Safety Policy (including Acceptable User Agreements)

This policy must be read in conjunction with Future Generation Trust's Safeguarding Policy and Behaviour Policy

1. Contents

2. Version control

Date	Version	Revision	Owner
19/09/17	1.0	New policy	Future Generation Trust Policy Team

3. Introduction

'Online actions can have offline consequences'

Future Generation Trust is committed to ensuring all pupils become safe and responsible users of existing and new technologies. We promote partnership with parents to achieve this goal by providing relevant and current guidance. This is achieved through:

- regular inclusion of material in newsletters
- annual parents' e-safety meetings
- information on academy websites
- involvement in high profile events such as Safer Internet Day
- providing copies of pupils' Acceptable User Agreements

By raising awareness of the risks associated with ICT, we hope to encourage pupils to access social media, the Internet and mobile phones in a safe and appropriate manner.

4. Aims

- To safeguard pupils and staff
- For all academy staff to recognise that e-safety is part of the 'duty of care', which applies to everyone working with pupils
- To raise awareness of the importance of e-safety amongst all staff so that they are able to educate and protect pupils in their care
- To inform staff how to manage their own professional reputation online and demonstrate appropriate online behaviours compatible with their role
- To educate and empower pupils so that they possess the necessary skills to make safe, responsible decisions and to feel confident to report any concerns that they have

5. Safeguarding

Inappropriate online contact is a high risk element of child protection. Potential issues such as cyberbullying and grooming are addressed in line with our Safeguarding Policy.

The Headteacher (Designated Safeguard Lead) or Deputy Designated Safeguard Lead will be informed immediately of any e-safety incidents involving Safeguarding concerns, which will then be escalated appropriately. They will record all reported incidents and actions taken in the academy's CPOMS Safeguarding system.

The academy will inform parents/carers of any incidents of concern as and when required.

Where there is a cause for concern or fear that illegal activity has taken place or is taking place, then the academy will contact the Children's Safeguarding Team for advice and/or escalate the concern to the Police. The Police will be contacted if a criminal offence is suspected.

6. Teaching and E-safety

Future Generation Trust ensures that all pupils receive an age appropriate input on e-safety each year throughout our ICT curriculum. Underpinning the curriculum are the SMART rules which are reinforced in school across the curriculum:

- **Safe** - encourages young people to be safe by not giving out their personal details online
- **Meeting** - draws attention to the risks associated with meeting someone you only know online
- **Accept** - highlights the risks of accepting emails, pictures and text messages from unknown sources
- **Reliable** is a reminder that not all information found online is necessarily reliable
- **Tell** - encourages children to tell someone if something happens or they meet someone online that makes them feel uncomfortable, or if they or someone they know is being bullied online.

E-safety understanding is provided in the following ways:

- A planned e-safety curriculum is provided as part of Computing / PSHE and is regularly revisited
- Key e-safety messages are reinforced as part of a planned programme of assemblies
- Pupils are encouraged to check authenticity and validate online content
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the Internet

7. Technical

The ICT technician is responsible for: ensuring that the academy's technical infrastructure is secure and is not open to misuse or malicious attack; that the academy meets required e-safety technical requirements and any Local Authority guidance that may apply; and that the use of the network is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher for action.

8. Photographic Images

We educate pupils about the risks associated with the taking and sharing of images, in particular, the risks attached to publishing their own images on the internet e.g. on social networking sites.

The Headteacher will inform parent(s)/carers(s) and others present at academy events that photographs/videos may be taken on the basis that they are for their personal use / private retention and not for publication in any manner.

This code of conduct specifies the manner in which Future Generation Trust academies will use and make available photographic images of pupils. Each academy will:

- Not use photographs in any form of internal or external publication where there is written objection from a parent/guardian.
- Not use photographs of pupils in swimwear.
- Not reveal within the image personal details, such as full pupils' names, date of birth, home address or telephone number.
- Not use any photographs of individual children either on its web site or Twitter account unless permission is sought.
- Not use photographs when children are wearing their night attire on school visits.

Parents will receive annual reminders to review the photographic consent they provide for their child. They have the option to inform the academy that they do not provide their consent using the form available on the academy website. Where a form is not submitted, it will be assumed that consent is provided.

Images taken on iPads for EY learning journeys are only to be taken in indoor classrooms and the outdoor areas (i.e. where another staff member is in the vicinity).

It is acceptable for staff to use mobile phones to upload messages to Twitter, relating to academy activities. Staff must then remove the images as soon as the message is live.

9. Social Media

When accessing and using social media for either professional or personal use, academy staff must ensure that they conduct themselves in a way which reflects positively on the academy.

Professional Use – Academy Twitter Account

Future Generation Trust is committed to the use of social networking sites for educational purposes and this is reflected by the number of users who follow the academy on Twitter.

Academy staff are authorised to post messages / images (in accordance with our Photographic Images Code of Practice) on the school's Twitter account in order to communicate general information to parents / carers and promote its educational activities. The protection of pupils, the academy and the individual when publishing any material online is paramount.

These communications may only take place on official (monitored) academy systems. Personal email addresses, text messaging or social media must not be used for these communications.

Notice and Take-Down Policy - Should it come to the academy's attention that there is a resource which has been inadvertently uploaded, and is inappropriate, or the academy does not have copyright permission to use that resource, it will be removed within one working day. Any digital communication between staff and parents / carers must be professional in tone and content.

Personal Use

It is important to note that once a comment is posted on social media, it ceases to be private.

The expression of opinion on web blogs, social networks or similar sites could inadvertently reveal information which is not suitable for public consumption and staff should be mindful of this and ensure they do not engage in inappropriate behaviour.

It is expected that staff do not make academy related comments or provide school information in social media. These include issues such as:

- Personal opinions about the academy
- Personal discussions about colleagues
- Information or opinions of parents / pupils
- Do not accept 'friend/follow' requests from a parent / pupil or former pupil of school age
- Do ensure privacy settings are appropriately used and checked regularly
- Do not access social media during work time, other than the academy Twitter account

By following this code, the wide variety of potential issues that some professionals have encountered will be avoided:

- Remove yourself if you have previously accepted a friend request from a pupil or their family members, who you only know through professional work.
- Other users could post a photo on their profile in which you are named, so think about any photos you appear in. On Facebook, you can 'untag' yourself from a photo.
- If you do find inappropriate references and/or images of yourself posted by a 'friend' online, you are advised to contact them and the site to have the material removed.
- Any adverse, abusive, threatening or defamatory comments must be reported to the Headteacher who will follow Local Authority and Staffordshire Police guidelines given below:

"If any parent does post malicious comments about the academy or staff, the first port of call would be to talk to the parent and explain why it's inappropriate; that it is harassment which is causing alarm and distress. Police advice is to put this in writing following the meeting with the parent. If it persists they can be banned from the school grounds and the police will be contacted as they are continuing to commit an offence according to section 5, 4 and 4a of the Public Order Act."

10. Cyberbullying

Cyberbullying can be defined as bullying via mobile phone or online (e.g. email, social networks and instant messenger). Future Generation Trust will ensure that:

- Cyberbullying (along with other forms of bullying) will NOT be tolerated.
- All incidents of cyberbullying reported to the academy, will be recorded on the academy's CPOMS Safeguarding System.
- Where bullying outside school is reported to the academy, it will be investigated and acted upon.

11. Mobile Phones

Pupils and Mobile Phones

It may be necessary for a child to have a mobile phone in school. If this is the case it must be switched off.

If a child uses a mobile phone for any of its functions whilst at school without permission from a member of staff it is to be confiscated. It should then be switched off in front of the pupil and taken to an office where it will be locked in a drawer.

Staff should not switch the phone on and check content.

If a member of staff is made aware that a pupil has a mobile phone in school but has not been using it then this should be reported to the Headteacher or Deputy Headteacher who will contact parents.

If an accusation is made that a pupil has shown other pupils "inappropriate material" then the phone should be confiscated, switched off and the SIM card removed. These will be kept in a locked drawer and the matter will be investigated by the Headteacher or Deputy Headteacher.

Sexting is described as 'youth produced sexual imagery' by children under the age of 18. Pupils will be encouraged to report all incidents of sexting. Teaching staff will inform the Designated Safeguarding Lead who will act according to the Safeguarding Policy and the guidance outlined in 'Sexting in schools and colleges: Responding to incidents and safeguarding young people'.

Staff and Mobile Phones

Personal phones should be kept out of sight of pupils and on a silent setting. Mobile phones can be used in class ONLY to send Twitter messages.

Texting and phone calls during lesson time and play duties are for emergencies only and staff should inform the Headteacher or Deputy Headteacher.

All other contact during the school day should be through the office.

12. Radicalisation and Extremism

Future Generation Trust ensures pupils are safe from terrorist and extremist material when accessing the internet in school, this includes establishing appropriate levels of filtering. If a concern arises pupils will know who to go to and adults should inform the Designated Officer for Safeguarding who will act according to the Safeguarding Policy and the guidance outlined in the Prevent and Channel Duty Guidance. The curriculum will ensure pupils are prepared positively for life in Modern Britain.

13. Monitoring and Review

The Future Generation Trust Board has overall responsibility for this policy and for reviewing its implementation and effectiveness. The Headteacher has day-to-day operational responsibility for the policy and must ensure that that are fully aware of its contents and trained accordingly.

This policy and all arrangements for E-safety will be reviewed annually.

Policy adopted on:	**4 October 2017**
Review Date:	**September 2018**

Signed: Fliss Dale **Designation:** Chair of Trust Board

Future Generation Trust

Acceptable User Agreement – for younger pupils (Foundation / KS1)

This is how we stay safe when we use computers:

I will ask a teacher or suitable adult if I want to use the computers / Ipads.

I will only use websites that my teacher has chosen.

I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong.

I will tell a teacher or suitable adult if I see something that upsets me on the screen.

Signed (child):……………………………………………

Future Generation Trust

Acceptable User Agreement – for older pupils (KS2)

I will only access computers with my login.

Safe

- I will tell my teacher about any unpleasant material or messages I find or are shown to me
- I will not give out my own details such as my name, phone number or home address.
- I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.
- I will make sure that all ICT contacts with other children and adults are responsible, polite and sensible.

Send

- I will not send to children or adults anything that could be considered unpleasant or nasty.

Save

- I will not save anything that could be considered unpleasant or nasty.

Search

- I will ask permission from a teacher before using the Internet

Signed (child):…………………………………………

Future Generation Trust

Acceptable User Agreement – Staff (and volunteers)

ICT and the related technologies such as email, the Internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the academy E-Safety Coordinator.

- I will only use the academy's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the academy or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role
- I will not give out my own personal details, such as mobile phone number and personal email address, to pupils
- I will only use the approved, secure email system(s) for any academy business.
- I will ensure that personal data (such as data held on SIMS) is kept secure and issued appropriately, whether in school, taken off the academy premises or accessed remotely.
- I will not browse, download, upload or distribute material that could be considered offensive, illegal or discriminatory.
- Images of pupils will only be taken and used for professional purposes in line with academy policy and will not be distributed outside the academy network without consent of the parent/ carer.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to the Headteacher.
- I will respect copyright and intellectual property rights.
- I will support and promote the school's e-Safety Policy and help pupils to be safe and responsible in their use of ICT and related technologies.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I agree to follow this code of conduct and to support the safe use of ICT throughout the school

Staff Signature .... Date ....

Print Name ....