

E-Safety Policy

School E-Safety Co-ordinator: Dan Oliver
Policy approved by Headteacher: September 2021
Policy approved by Governors: October 2021
Policy review frequency: Every 2 years
Date of next review: September 2023

Contents

Cover	Page 1
Contents	Page 2
1. Rationale & Approach	Page 3
2. Principles	Page 5
3. Information Systems and Security	Page 5
I. Filtering	Page 5
II. Computer Activity	Page 6
III. Email	Page 6
IV. Assessing Risk	Page 6
4. Reporting and Responding to incidents of Misuse	Page 7
5. Use of Digital and Video Images	Page 7
6. Social Media – Protecting Professional Identity	Page 7
7. Personal Data	Page 8
8. Roles and Responsibilities	Page 8
Appendix	Page 10
Acceptable Use Policy	
Online Safety Recommendations for Parents	
ICT Acceptable Use Policy for Students at Home	
Guidance for Video Conferencing	

1. Rationale

What do we mean by E-Safety?

E-Safety is about safe and responsible use of modern technology to include:

- existing and future stationary/mobile electronic devices;
- existing and developing Internet-based technologies, used for the purposes of learning, business and recreation.

The Futures Trust Academy and all schools within the Trust believes a clear e- safety policy, consistently and fairly applied, underpins effective education. The use of the internet and connected devices pose a risk to the safety of the young people in our care. The Trust will ensure that all school staff, students and parents are all clear of the high standards of behaviour expected at all times.

The school recognises the benefits and opportunities which new technologies offer to teaching and learning. We provide internet access to all learners and staff and encourage the use of technologies in order to enhance skills, promote achievement and enable lifelong learning. This includes the use of video conference technology for remote teaching such as Microsoft Teams (see Appendix). However, the accessibility and global nature of the internet and different technologies available mean that we are also aware of potential risks and challenges associated with such use.

Approach to addressing risks

Our approach is to implement appropriate safeguards within the school, while supporting staff and students to identify and manage risks independently and with confidence. Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in e-safety is therefore an essential part of the schools' e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience. We believe this can be achieved through a combination of security measures, training, guidance and implementation of our policies.

In furtherance of our duty to safeguard students, we will do all that we can to make our students and staff stay e-safe and to satisfy our wider duty of care. E-safety will be a focus in all areas of the curriculum and staff should take active steps to reinforce e-safety messages across the curriculum.

The Relationships, Sex & Health Education (RSHE) policy outlines the way students are supported to learn about healthy relationships, mental health, physical health, safeguarding & exploitation, democracy. E-safety is a theme that runs throughout these modules. There is also a module each year focussing on "online and media" specifically.

The following areas of risk highlighted by Keeping Children Safe in Education are the main concerns addressed by this policy and throughout the 7 year journey our students take at Barr's Hill:-

- “• content: being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
- contact: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes’.
- conduct: personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying; and
- commerce - risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (<https://apwg.org/>).”

This e-safety policy should be read alongside other relevant school policies, including:

- Safeguarding and Child Protection
- Guidance for Safety Working Practice
- Dealing with Allegations of Abuse Against Staff and Volunteers
- Whistleblowing Policy
- Acceptable Use Policy
- Behaviour Policy

2. Principles

This policy applies to all members of the school community (including staff, students, volunteers, parents/carers, visitors and community users) who have access to and are users of the school's ICT systems, both in and out of the school.

The Education and Inspections Act 2006 empowers head teachers, to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other e-safety incidents covered by this policy, which may take place outside of the school but are linked to membership of the school.

The school will deal with such incidents within this policy, and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate e-safety behaviour that take place out of school. In order to safeguard our community external agencies including the Police may also become involved.

3. Information Systems and Security

The security of the school's information systems, and users, will be reviewed regularly and as follows:

- Virus protection will be updated regularly;
- Academy computer activity will be monitored through RADAR, formerly known as (Policy Central Enterprise or PCE) and concerns alerted to the Designated Safeguarding Leads
- Unapproved software will not be allowed in students' work areas or attached to email;
- Files held on the school's network will be regularly checked;
- The network manager will review system capacity regularly.

I. Filtering

The Trust will work with all schools to ensure that systems to protect students are reviewed and improved. The network manager will regularly review and update filtering systems every term or as is required. If staff or students discover unsuitable sites, the URL must be reported to IT Services immediately. The school's broadband access will include filtering appropriate to the age and maturity of students. Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable. Any material that the school believes is illegal must be reported to appropriate agencies such as IWF or CEOP.

II. Computer Activity

All Trust computers have RADAR software installed. The purpose of RADAR is to enable the School to enforce its own Acceptable Use Policy (AUP) and control misuse of computing resources. RADAR software flags inappropriate activity and these reports are passed to the DSLs depending on the level of the concern on the same day by the Warwickshire based RADAR team. The software has a number of e-safety features such as desktop filtering, website logging, categorised scanning (using keyword libraries), AUP display, Internet and application time management and all web activity monitoring.

III. Email

Email usage and accounts will be monitored closely to reflect the school's high standards:

- Students may only use approved email accounts;
- Students must immediately tell a teacher if they receive offensive email;
- Students must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult;
- Excessive social email use can interfere with learning and will be restricted;
- Email sent to external organisations should be written carefully, in the same way as a letter written on school headed paper;
- School' may have a dedicated email for reporting wellbeing and pastoral issues and this inbox must be approved and monitored by the Designated Safeguarding Lead;
- Staff should only use school email accounts to communicate with students as approved by the Senior Leadership Team;
- Staff should not use personal email accounts during school hours or for professional purposes.

IV. Assessing Risk

The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. The school will audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate. The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990. Methods to identify, assess and minimise risks will be reviewed regularly.

4. Reporting and Responding to Incidents of Misuse

The staff and student AUP set out the requirements in relation to the reporting of unsuitable or inappropriate activities. Where such activities also raise a safeguarding concern, the school's Child Protection and Safeguarding Policy and relevant procedures must be followed.

It is more likely that the school will need to deal with incidents that involve inappropriate, rather than illegal, misuse. Incidents will be dealt with as soon as possible in a proportionate manner and members of the school community will be made aware that incidents have been dealt with. Incidents of misuse will be dealt with through normal behaviour and disciplinary procedures.

5. Use of Digital and Video Images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents and carers and students need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyber bullying and/or exploitation to take place.

Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is increasingly common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm.

The Privacy Notice Policy and the Data Protection Policy are used to ensure that students, parents/carers and staff understand the way school may use digital and video images.

Parents and Carers can opt out of their child's image being used digitally in school.

6. Social Media – Protecting Professional Identity

The AUP sets out the expectations about the appropriate use of social media by staff, students and parents/carers. This guidance must be followed in order to ensure that staff, students and parents/carers do not engage in any activity which may cause them to breach acceptable standards of conduct.

7. Personal Data

The Futures Trust ('the Trust' includes all schools within the Trust) aims to ensure that all personal data collected about staff, pupils, parents, trustees, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA 2018). This policy applies to all personal data, regardless of whether it is in paper or electronic format.

For more information please refer to the Privacy notice and Data Protection Policy on the school website.

8. Roles and Responsibilities

The following section outlines the broad e-safety roles and responsibilities of individuals and groups within the school.

The School Governors

The School Governors are responsible for the overall effectiveness of the policy. This will be carried out by the Governing Body receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has the role of Safeguarding Link, which includes e-safety.

The Headteacher and Senior Leadership Team

The Headteacher has a duty of care for ensuring the safety of members of the school community and therefore has overall responsibility for e-safety in the school.

E-safety Co-Ordinator

The Headteacher delegates much of the day to day responsibility for e-safety to an E-Safety co-ordinator who may often also be the Designated Safeguarding Lead (DSL). The E-Safety Co-ordinator has a leading role in establishing, reviewing and implementing the school e-safety procedures, providing training and advice for staff and liaising with outside bodies in relation to e-safety issues.

Students

Students should be aware of the significant risks of exposing themselves or others to personal harm or danger because of inappropriate use of IT and digital media and should manage their use of IT to minimise these risks.

Students are responsible for using the school IT systems in accordance with their AUP, and generally understanding the importance of adopting good e-safety practice when using digital technologies in and out of school.

Parents and carers

Parents and Carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. This includes home learning and remote teaching, such as the use of Video Conferencing (see Appendix).

The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, the school website and information about national and local e-safety campaigns and literature.

Staff

Staff are responsible for ensuring that they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices (including guidance for video conferencing) and have read, understood and signed the staff Acceptable Use Policy (AUP). Staff that work directly with students are also responsible for helping them understand the importance of e-safety and how they can reduce exposing themselves to risk.

IT Support

IT Support (specifically the network manager) is responsible for ensuring that the school's technical infrastructure is secure and is not open to misuse or malicious attack and has all the necessary controls in place, such as web filtering and password protection to reduce the risk of e-safety issues arising.

HR

HR monitor staff usage of the internet

Appendix

ICT Acceptable Use Policy for Students

Introduction

Technology and the internet are powerful tools, which are integral to life in and out of school. They can be used in very positive ways to enhance learning or for negative purposes such as cyber-bullying or promoting division and extreme viewpoints. PRIDE values of “Pro-Active, Responsible, Inquisitive, Determined, Engaged” apply just as much to online behaviours.

This Acceptable Use Policy is intended to ensure, that at all times:

- Young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- School systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

The school will try to ensure that students will have good access to digital technologies to enhance their learning and will, in return, expect the students to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must act in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the school ICT systems and other users.

For my own personal safety:

- I understand that the school will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person’s username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will be aware of “stranger danger”, when I am communicating on-line.
- I understand that there may be times when someone tries to gain my trust on-line in order to persuade me it is safe to give them access to personal information, images/video, social media accounts or data. I will report any attempts to a trusted adult.
- I understand not all information online is reliable, including fake people and fake news.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc)
- I will not arrange to meet people off-line that I have communicated with on-line without parental knowledge and accompanied by an adult.

- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- I will not try (unless I have permission) to make large downloads or uploads.
- I will not use the school systems or devices for chat rooms, social media, pornography, violent or extreme content, on-line gambling, internet shopping or file sharing
- I will not use the school systems for on-line gaming or video broadcasting (eg YouTube), unless I have permission of a member of staff to do so.

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

- I will not use any personal devices, including USB devices, in school without first asking permission and understand any mobile phone seen on school site is liable to be confiscated, until collected by a parent.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person / organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.
- I will **NOT** use social media on school site, or at all using school equipment.
- Where work is protected by copyright, I will not try to download copies (including music and videos)

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the school network / internet, detentions, exclusions, contact with parents and in the event of illegal activities involvement of the police.

User's Acceptance

By clicking "Accept" I acknowledge that I have read and understood the acceptable use policy and agree to abide by the requirements laid down.

Staff Acceptable Use Policy

This is available as a separate but related policy.

Online Safety Recommendations for Parents

Students safety is our first priority and everyone's responsibility. Please follow the below guidelines to help keep young people safe online.

If you have any concerns, please contact school, see the website for details.

Please go through the "**Student Acceptable Use Policy for Home Learning**" (below) with your child.

Please **discuss regularly** with your child all aspects of their experience online, not just their learning, social media and gaming too. Please ask them key questions, reassure them you want to learn and understand their online world, not to judge or criticise them. Small and often is usually better than a big one off "talk"!

"Which apps are popular in your year? What are the best/worst things about social media? How does it impact young people's mental health? What are the riskiest things people your age do online? What would you say to one of them if they asked you for advice on some of those risks?"

Use **Parental Controls** (see below), so that you protect young people from websites that use pop-ups, advertising or harmful content such as pornography, hateful or extremist propaganda, online fraud, gambling or other addictive activities. This will reduce risks but will not eliminate them as no filters are a substitute for supervision.

Supervision and monitoring by a parent is not always possible, but it is the best way to ensure your child does not end up on websites or applications that might try and engage them in inappropriate content. Please consider having no screens in bedrooms, especially at night, setting agreed and reasonable boundaries on screen time and trying to find a balance that works for your family!

We use Microsoft Teams for setting homework, streaming assemblies and some "live" remote teaching. These are recorded to enable us to follow up any issues or concerns that may arise and understand how we can develop best practice.

There is a wealth of **useful information** to support you as follows. Please also see the safeguarding page on the school website.

Setting up parental controls, age specific advice
Making a Family Agreement on Screen Time
Learning about games, apps, websites

www.internetmatters.org
www.childnet.com/parents-and-carers
www.common sense media.org/

ICT Acceptable Use Policy for Students at Home

I understand that I must act in a responsible way, to ensure that there is no risk to my safety or to the safety and security of my home network or the school ICT systems and other users.

For my own personal safety:

- I understand that the school expect my parent/carers to monitor my use of the systems, devices and digital communications, at home;.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will be aware of "stranger danger", when I am communicating on-line.
- I understand that there may be times when someone tries to gain my trust on-line in order to persuade me it is safe to give them access to personal information, images/video, social media accounts or data. I will report any attempts to a trusted adult.
- I understand not all information online is reliable, including fake people and fake news.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc)
- I will not arrange to meet people off-line that I have communicated with on-line without parental knowledge and accompanied by an adult.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I will act as I expect others to act toward me:

- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.
- I understand that some online content is illegal such as any explicit images of under 18s. Violent, hateful, racist, or prejudiced views against other groups may also be illegal or upsetting and I will not access, share, like or respond to any inappropriate content.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person / organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).

Student Name
Parent Name

Year
Date

Guidance for using Video Conferencing

Safeguarding and child protection remains as important in this environment as anywhere else, and staff members should apply their school's safeguarding policies, guidance and procedures to online learning, just as they would to classroom working - staff who are concerned about a child's welfare or have concerns for a child's safety should without delay, follow their school's safeguarding procedures.

The school will inform parents and carers of the platforms that pupils/students are being asked to use, what they will be asked to do online and which members of staff they will be interacting with.

The following guidance is from the Virtual School Guidance for staff

- You must record the lesson. This is key for safeguarding and also has the advantage that students can watch it again after or if they were unable to attend. There will not be a second adult in the lesson (if there is, you must inform students). If a student misbehaves – remove them from the lesson and report it to the hub director. The member of SSD will also be on call at this time.
- If a student makes a disclosure or you have a safeguarding concern report this in the normal way. If urgent, contact Dan Oliver directly and then report on CPOMs. If non-urgent report on CPOMs.
- Ensure you are appropriately dressed & wear your ID badge.
- Consider the environment you are recording in, for example, which room, what or who is in the background? Is it quiet and 'professional'?
- Blur the background on your screen, only use agreed logos as "profile pictures"
- Staff must use school equipment/platforms (no social media) unless you have specific permission
- Any third-party material you post on Teams must be viewed before recommending and be from reputable sources
- No 1-1 video conference with students & no sharing of personal information
- Safeguarding script (below) must be read out at the start of every tutorial.

"Before we start, we will outline basic expectations for the lesson. Please ensure your background is blurred and your mic is switched off until you need to ask a question/respond. As with any lesson, usual PRIDE standards are expected, but in this new learning environment, you may have to be extra patient with staff and other students, as we all work together to make this effective learning time. A few specifics:

- *Please note the IT Acceptable Use Policy applies, as in school, and has been posted on the website, emailed out to students and parents.*
- *Please dress appropriately.*
- *You can choose not to turn "video" on if you feel more comfortable with audio only.*
- *Respect other people's consent and privacy, don't record, share or criticise.*
- *Try to make sure no one else is in the background of your video or anyone's personal information is on show.*
- *Staff and students will follow the normal safeguarding policies, so if anyone has a concern, staff will share it with the safeguarding team so that support can be put in place. If you are*

worried about anything you can contact any staff member or ChildLine if you prefer on 08001111. Please bear in mind staff will record sessions, but we would ask students not to use this feature please.

- There will likely be a short delay at times, depending on internet loads, so try not to talk over people where possible.”

Further information can be found at:

<https://learning.nspcc.org.uk/news/2020/march/undertaking-remote-teaching-safely/> <https://swgfl.org.uk/resources/safe-remote-learning/>

[https://www.gov.uk/guidance/remote-education-practice-for-schools-during-coronavirus-covid-19?utm_source=68f634af-e3d5-455f-bd99-](https://www.gov.uk/guidance/remote-education-practice-for-schools-during-coronavirus-covid-19?utm_source=68f634af-e3d5-455f-bd99-6ae7e8aa4d13&utm_medium=email&utm_campaign=govuk-notifications&utm_content=immediate)

[6ae7e8aa4d13&utm_medium=email&utm_campaign=govuk-notifications&utm_content=immediate](https://www.saferrecruitmentconsortium.org/GSWP%20COVID%20addendum%20April%202020%20final-1.pdf)
<https://www.saferrecruitmentconsortium.org/GSWP%20COVID%20addendum%20April%202020%20final-1.pdf>

<https://www.gov.uk/guidance/safeguarding-and-remote-education-during-coronavirus-covid-19>