Policy Information Sheet

Name of Policy:	**Online Safety Policy**
Delegated Authority	☒ Trust Board ☐ Nominated Committee ☐ CEO ☐ CFO ☐Other _____
Policy review cycle	☒ Annual ☐ 3 years ☐ 4 years ☐ Other
Statutory policy	☒ Yes ☐ No
Published online	☒ Statutory ☐ Trust recommended ☐ No

Document Control	
Created by (author)	Lorna McLean
Date created	08/05/2024
Approved by	Trust Board
Date approved	May 2024
Next Review Date	October 2027
Recorded in minutes	

Document History			
Version	Author	Revisions	Final approval date
1.0	Lorna McLean		July 2025
2.0	R.Kitson	No changes	06.10.2026

Contents

1. Aims 3
2. Legislation and guidance 4
3. Roles and responsibilities 4
4. Educating students about online safety 6
5. Educating parents about online safety 8
6. Cyber-bullying 8
7. Acceptable use of the internet in school 10
8. Students using mobile devices in school 11
9. Staff using work devices outside school 11
10. How the school will respond to issues of misuse 11
11. Training 11
12. Contacting students during the school day 132
13. Use of social networking and online media 12
14. School practice 13
15. Links with other policies 13
16. Monitoring arrangements 13
Appendix 1: acceptable use agreement (students and parents/carers) 14
Appendix 2: acceptable use agreement (staff, Trustees, volunteers and visitors) 15

1. Aims

Make It Different: Principles and Values

Make It Different exists to build on the high-quality work of Spark of Genius North-East, specifically King Edwin School. The Trust has been established, initially to operate the new Hartlepool SEMH Free School (HFS). The school will operate within the guiding values of;

- Kindness
- A Growth Mindset
- Resilience
- Personal Responsibility

Our core beliefs and mission are as below;

Parental confidence and trust

Building trust with families is important and helps children to feel secure in their learning. We will work hard with all parents and carers to ensure we build a team around each young person together.

Emotional resilience and well-being

We will help our students understand and process their emotions effectively and teach them how to do this themselves. We will also help our students learn how to deal with the challenges they will come across in learning and in life.

Personal progress and achievement

It is our aim that every child will leave the school with a qualification in English and mathematics, with other qualifications chosen to suit each student and their needs and next steps.

Preparing for adulthood

We will work hard to make sure our students are well prepared for their next steps, and that they are well informed about their options. We will provide meaningful work experience, in school apprenticeships and internships, employer visits and contact, and lots of opportunity to explore the whole range of post 16 options to our students starting from their first days with us.

Children have a sense of belonging in the community

We will make sure there are lots of opportunities for our students to get involved in community activity, both in school and out of school. We will encourage involvement in our Duke of Edinburgh programme, and encourage our students to think about others, both people they know and people they do not.

Staff confidence and competence – greater capacity to meet needs We will support our staff to be well trained, confident, competent and able to think about how to develop their skills further. We will offer good quality staff training and development throughout the year, making sure that staff use new knowledge to develop and improve what they do on a day-to-day basis.

British Values

All staff are expected to uphold and promote fundamental British Values including democracy, the rule of law, individual liberty and mutual respect and tolerance of those with different faiths and beliefs.

1.1 Make It Different Trust aims to:

- have robust processes in place to ensure the online safety of students, staff, volunteers and Trustees

- deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- establish clear mechanisms to identify, intervene and escalate an incident, where appropriate
- ensure that our online safety policy reflects the overall ethos and values of the school
- encourage students to maximise the benefits and opportunities that technology has to offer
- ensure that students learn in an environment where security measures are balanced appropriately with the need to learn effectively
- equip students with the skills and knowledge to use technology appropriately and responsibly
- teach students how to recognise the risks associated with technology and how to deal with them, both within and outside the school environment
- ensure that all users in the school community understand why there is a need for an Online Safety Policy.

2. Legislation and guidance

2.1 This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department's guidance on protecting children from radicalisation.

2.2 It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on students' electronic devices where they believe there is a 'good reason' to do so.

2.3 The policy also takes into account computing within the curriculum which complies with our funding agreement and articles of association.

3. Roles and Responsibilities

3.1 The Trust Board

The Trust has overall responsibility for monitoring this policy and holding the Principal Designate to account for its implementation. Through its committee structure, it will monitor senior leaders and staff and discuss online safety, and online safety logs as provided by the designated safeguarding lead (DSL).

Trustees will:

- Ensure that they have read and understood this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 2)
- Meet regularly with the DSL/HT to monitor the effectiveness of online filtering and monitoring systems in line with KCSIE.

3.2 The Principal

The Principal is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

The Principal and DSL should be aware of procedures to be followed in the event of a serious safeguarding allegation made against a member of staff if an incident of online misuse should occur.

3.3 The Designated Safeguarding Lead (DSL)

Details of the school's Designated Safeguarding Lead (DSL) and deputies are set out in our child protection and safeguarding policy.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the Principal in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Principal, IT Support services and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy and that there are instant and effective system in place to investigate and manage online safety concerns from Securly Alerts and notifications.
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the Principal
- Ensuring that any online safety incidents are logged on CPOMS by DSL and/or relevant staff appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Review the filtering monitoring provision at least annually.

3.4 IT Support Service

The IT support service provider is responsible for:

- Providing an appropriate filtering and monitoring solution for the school to procure.
- Maintaining the filtering and monitoring systems and making sure they are working as expected in order to keep students safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Providing documentation on what is blocked or allowed and why.
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a specified basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that servers, wireless systems, and cabling must be securely located and physical access restricted.
- Providing all users with a username and secure password. The service provider will keep an up-to-date record of users and their usernames. Users are responsible for the security of their username and password and must not share this with anyone else.
- Providing filtering and monitoring reports including alerts which will be sent to DSL staff. Users are made aware of this in the Acceptable Use Agreement (Securly Filtering and Monitoring reports along with the online portal and alerts are used to monitor and record activity)
- Working with the SLT and DSL to carry out review and checks.

This list is not intended to be exhaustive.

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 2), and ensuring that students follow the school's terms on acceptable use (appendix 1)
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

We have a Securly online filtering and monitoring system on all school devices. The HT works alongside the IT Service Provider to review the systems to safeguard students and staff. Filtering and monitoring systems are both important parts of safeguarding students and staff from potentially harmful and inappropriate online material.

3.6 Parents

Parents are expected to:

- Notify a member of staff or the Principal Designate of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendix 1)

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues?, UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues
- Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics
- Parent factsheet, Childnet International: http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf

3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 2).

4. Educating students about online safety

4.1 Students will be taught about online safety as part of the curriculum.

In the **Primary phase**, students will be taught to:

- understand what online safety means and the possible risks associated
- understand what can be accessed online, including an introduction to social media
- develop their awareness and understanding of how to stay safe online

In **Key Stage 3**, students will be taught to:

- understand a range of ways to use technology safely, respectfully, responsibly, and securely, including protecting their online identity and privacy

- recognise inappropriate content, contact and conduct, and know how to report concerns

Students in **Key Stage 4** will be taught:

- to understand how changes in technology affect safety, including new ways to protect their online privacy and identity

  how to report a range of concerns

4.2 The safe use of social media and the internet will also be covered in other subjects where relevant. The school will raise students' awareness of the dangers that can be encountered online and may also invite speakers to talk to students about this.

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' online safety and digital literacy is therefore an essential part of the school's online safety provision.

Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience and awareness. Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum should be provided as part of Computing and other relevant lessons and should be regularly revisited and monitored.
- Key online safety messages should be reinforced as part of a planned programme of talks and tutorials / pastoral activities
- Students should be taught in all lessons to be critically aware of the materials and content that they access on-line and be guided to validate the accuracy of information.
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making
- Students should be helped to understand the need for the student / student Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside of school.
- Staff should act as good role models in their use of digital technologies and the internet.
- In lessons where internet use is pre-planned, it is best practice that students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- Where students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit. This is supported by effective Securly filtering and monitoring.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need and discussed with the DSL.

5. Educating parents about online safety

5.1 The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website and social media accounts. This policy will also be shared with parents.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the DSL or relevant member of staff.

Concerns or queries about this policy can be raised with the school.

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power.

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that students understand what it is and what to do if they become aware of it happening to them or others. We will ensure that students know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with students, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, Trustees and volunteers (where appropriate) receive training on cyber bullying, its impact and ways to support students, as part of safeguarding training.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in in the peer on peer abuse policy.

Where illegal, inappropriate or harmful material has been spread among students, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

6.3 When responding to cyberbullying concerns, the school will:

- Act as soon as an incident has been reported or identified.
- Provide appropriate support for the person who has been cyberbullied and work with the person who has carried out the bullying to ensure that it does not happen again.
- Encourage the person being bullied to keep any evidence (screenshots) of the bullying activity to assist any investigation.
- Take all available steps where possible to identify the person responsible. This may include looking at use of the school systems; identifying and interviewing possible witnesses; contacting the service provider and the police, if necessary
- Work with the individuals and online service providers to prevent the incident from spreading and assist in removing offensive or upsetting material from circulation. This may include supporting reports to a service provider to remove content if those involved are unable to be identified or if those involved refuse to or are unable to delete content.

- Confiscate and search students' electronic devices, such as mobile phones, in accordance with the law and DfE guidance 'Searching, screening and confiscation at school' and Childnet Cyberbullying guidance to ensure that the school's powers are used proportionately and lawfully.

- Request the deletion of locally-held content and content posted online if they contravene school behavioural policies.

- Provide information to staff, parents and students regarding steps they can take to protect themselves online. This may include advising those targeted not to retaliate or reply, providing advice on blocking or removing people from contact lists or helping those involved to think carefully about what private information they may have in the public domain.

6.4 Parents should:

- report any bullying to the relevant social media site (e.g. Facebook/Twitter) and to the Police
- keep any evidence, e.g. the message or a screen print
- block or delete the person being abusive
- change their child's mobile phone number
- check the security settings and privacy settings on their child's account. These need to be updated regularly
- monitor their child's use of the internet, social networking and gaming sites, e.g. review their friend list; do they know who all of the people are? They would warn them against talking to strangers on the street so the same rules apply online
- make sure that their child is careful about who they give their contact details to. They might receive unwanted messages if they are part of a group
- ensure their child knows to tell a parent or teacher immediately if they receive an inappropriate image or video (such as a video of a fight taking place). If your child stores this video on their phone or computer, or even open it and delete it, they could find themselves in trouble with the Police at a later date
- make sure that their child understands that information they share online stays there forever. Deleting a message does not mean that it cannot be recovered by someone else at another time
- ensure that children under 13 do not have Facebook accounts
- not involve themself in any disputes by sending a message as they could then find themself in trouble with the Police. Report any issues to the relevant social media company as well as the Police.

The link below is full of resources, including advice on parental controls, checking privacy settings with children and lists of things to be aware of for different age groups. It also includes a digital magazine for all issues in their area:

- CEOP – www.thinkuknow.co.uk

6.5 Students should:

- use social media responsibly, e.g. not make rude, abusive or threatening comments to anyone
- only talk to people that they know and only accept friend requests from people they know to be friends
- not give out any personal information, e.g. address, phone number, email address. The same applies to online gaming
- never go and meet anyone they have met online (e.g. Lauren who is 15 could turn out to be Rob who is 45)
- be careful about who they give their contact details to. In being part of a group chat, they might receive unwanted messages, images or videos
- never share passwords or use anyone else's device when they are logged in on their account
- never download anything illegally, e.g. music

- be aware that comments made online or pictures posted are there forever. Deleting a message does not mean that it cannot be recovered by someone else at another time
- be aware that friends of friends may be able to see comments, photos and videos because of their privacy settings
- check their security settings and privacy settings regularly
- tell a parent or another adult if they experience online bullying
- tell a parent or another adult if they receive an inappropriate message, image or video (such as a video of a fight taking place). If they store this video on their phone or computer, or even open it and delete it, they could find themself in trouble with the Police at a later date
- report any abusive behaviour to the relevant social media site, but ensure they keep the evidence, then block or delete the person who has been abusive

6.6 Examining electronic devices

i. School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on students' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so. This should always be reported to the DSL immediately and no images or content to be deleted until a discussion with the DSL has taken place. Where there is a safeguarding concern, the device should be immediately confiscated until it can be investigated further by the DSL.

   Hartlepool Free School does not allow users to "Bring Your Own Device" and only allow authorised devices to have access to the schools network. All users should understand that the primary purpose of the use of mobile phones or devices by staff in school is for purely educational purposes.

ii. When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

   - Cause harm, and/or
   - Disrupt teaching, and/or
   - Break any of the school rules

iii. If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

   - Delete that material, or
   - Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
   - Report it to the police

iv Any searching of students will be carried out in line with the DfE's latest guidance on screening, searching and confiscation. Any complaints about searching for or deleting inappropriate images or files on students' electronic devices will be dealt with through the school complaints procedure.

7. Acceptable use of the internet in school

7.1 In using the school based computers, staff, students and other users click to agree the Acceptable Usage agreement. Staff also sign an agreement regarding the acceptable use of the school's ICT systems and the internet. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

7.2 Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

7.3 We will monitor the websites visited by students, staff, volunteers, Trustees and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements.

8. Students using mobile devices in school.

8.1 Students may bring mobile devices into school for staff to store safely in line with the Mobile phone policy, but are not permitted to use them on site, unless given express permission by a member of staff. This will be supervised by the member of staff who has given permission. Any breach of the acceptable use agreement by a student may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

8.2 Staff use of Mobile phones in school

The school operates as a mobile-free environment, except in cases of emergency, safeguarding requirements, or other authorised circumstances. Such as the whole school communication group

In line with the Department for Education guidance and Ofsted expectations, staff must not use mobile phones in classrooms or in any area where students are present and visible, including during breaktimes and lunchtimes, unless required for an emergency, safeguarding matter, or another authorised purpose.

Staff who need to access their mobile phone for personal or non-urgent matters must do so away from students, in a staff room, office, or other designated staff-only area.

Consistent adherence to this policy ensures that staff model the professional standards, behaviours, and expectations that we seek to promote throughout the school community.

9. Staff using work devices outside school

9.1 Staff members using a work device outside of school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use (see appendix 2).

9.2 Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted. If staff have any concerns over the security of their device, they must seek advice from the Head teacher. Work devices must be used solely for work activities.

10. How the school will respond to issues of misuse

10.1 Where a student misuses the school's ICT systems or internet, we will follow the procedures set out in the behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

10.2 Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident. The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training

11.1 All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

11.2 All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

11.3 The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

11.4 Trustees will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

11.5 More information about safeguarding training is set out in our child protection and safeguarding policy.

12. Contacting students during the school day

12.1 In accordance with the school's procedures, parents/carers should contact students only via staff in school.

13. Use of social networking and online media

13.1 The school asks its whole community to promote this approach to online behaviour:

- Common courtesy
- Common decency
- Common sense

13.2 How do we show common courtesy online?

- We ask for permission before uploading any content about someone else (photographs, images, videos, etc.)
- We do not write or upload hurtful, rude or derogatory comments or materials. To do so is disrespectful and may upset, distress, bully or harass

13.3 How do we show common decency online?

- We do not post comments that can be considered intimidating, racist, sexist, homophobic or defamatory. This is cyberbullying and may be harassment or libel.
- When such comments exist online, we do not forward the emails, tweets, posts or videos. By creating or forwarding such materials we are all liable under the law.

13.4 How do we show common sense online?

- We think before we click
- We think before we upload comments, photographs or videos
- We think before we download or forward any materials
- We think carefully about the information we share with others online, we check where it is saved and we check our privacy settings
- We make sure we understand any changes in use for any of the websites we use
- We block harassing communications and report any abuse – initial abusive messages should be saved as evidence before blocking the sender.

Social Media - Protecting Professional Identity

All schools and local authorities have a duty of care to provide a safe learning environment for students and staff. Schools could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, engage in online bullying, discriminate on the grounds of sex, race or disability, or who defame a third party may render the school liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

School provides the following measures to ensure reasonable steps are in place to minimise risk of harm to students and staff:

- Ensuring that personal information is not published
- Training is provided including: acceptable use; social media risks; checking of settings; data protection and reporting issues or concerns
- Clear reporting guidance, including responsibilities, procedures and sanctions are in place
- No reference should be made in social media to students / students, parents / carers or school staff where consent is not given
- Staff do not engage in online discussion on personal matters relating to members of the school community
- Security settings on personal social media profiles are in place as they may be regularly checked to minimise risk of loss of personal information

Any online actions that impact on the school that could potentially bring the school into disrepute will be responded to at the discretion of the Principal Designate.

14. School practice

14.1 The school uses social networking sites to share information with students and parents (e.g. school Facebook site). These sites are authorised by the school in advance of use and are therefore closely regulated.

15. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Promoting Positive Behaviour policy
- Staff HR policies and procedures
- Data protection policy and privacy notices
- Complaints policy

16. Monitoring arrangements

16.1 The DSL ensures any online safety incidents are logged and dealt with appropriately in line with this policy. Incidents will be logged on CPOMS if they relate to students. If the incident relates to a member of staff, it will be logged on CPOMS Staff Safe unless directed otherwise by the Principal Designate.

16.2 This policy will be reviewed annually by the CEO/CFO and then shared with the Trust Board.

Acceptable Use Policy for Students

Our computers have internet access to help our learning.

These rules will help keep us and our computer equipment safe.

When using the school's ICT systems and accessing the internet in school, I will not:

- Use them for a non-educational purpose
- Use them without a teacher being present, or without a teacher's permission
- Access any inappropriate websites
- Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity)
- Use chat rooms
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Share my password with others or log in to the school's network using someone else's details
- Give my personal information (including my name, address or telephone number) to anyone without the permission of my teacher or parent/carer
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

In addition:

I agree that the school will monitor the websites I visit.

I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others. I will always use the school's ICT systems and internet responsibly

I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for students using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Name of Student: _____ Class: _____

Signed by Student: _____ Date: _____

Signed by Parent/Carer: _____ Date: _____

Acceptable ICT Usage declaration

This document is in relation to:

- Any equipment loan and/or use of school IT or communications equipment
- School mobile devices
- Personal mobile devices used to access school work and/or emails

You are required to sign this document and a record of this declaration will be kept in school.

When logging on to the school network you must read and agree to the terms of usage each time you log on. This is deemed as the School's Acceptable ICT Usage Statement and by clicking OK you agree to be bound by the conditions as stated within this document.

Failure to abide by the requirements within this document could lead to disciplinary action. If you are unsure about ICT usage at any time, please speak to the Head teacher or CFO in the first instance.

Laptops and school mobile devices are owned by the school and are only to be used by staff to enhance their professional activities including teaching, research, administration and management. Please be aware that laptops and mobile devices are only to be used by the member of staff they are issued to, and may be subject to random checks by senior management.

Use of personal devices to photograph or record students is strictly prohibited. Only school devices loaned to staff may be used for this purpose, and only in order to enhance professional activities. Staff must ensure that permission has been previously received by the relevant students, prior to their photographs being taken.

When using social media, you must protect your personal information, and comply with the school's social media guidance.

It is required that all school equipment including computers, laptops and mobile devices:

- Should only be used for activities appropriate to staff professional needs.
- May only be used for personal use at the written discretion of the CFO without damaging the integrity of the school and school systems.
- Must never be used for accessing social media, other than to enhance professional activities.
- Must never be used for purchasing inappropriate materials such as pornographic, racist or offensive material, or for personal financial gain, gambling, political purposes, advertising, or accessing chat rooms.
- Should **only be used by the named person** signing this declaration. The person signing this declaration is solely responsible for any material accessed via the equipment, and to this end, will face disciplinary action should inappropriate use occur.
- Should only be accessible via a password, known only to the user and senior management of the school.

Please note

- The equipment remains the property of Make It Different Trust
- Insurance cover provides protection from the standard risks but excludes accidental damage and theft from an un-attended car. If the equipment is stolen from an un-attended car, you will be responsible for its replacement.
- Only software licensed by the school, authorised by the Head teacher or their representative and installed by the school's IT support service may be used.
- Anti-virus software which is installed on laptops must be updated on a weekly basis, with advice available from IT support on the routines and schedule of this operation.

- Should any faults occur the school's IT support service must be advised as soon as possible so that they may undertake any necessary repairs. Under no circumstances should staff attempt to fix suspected hardware/software faults.
- Training on how to access school systems will be provided by the IT support service.

When using personal devices to access school work and/or emails, the individual member of staff is personally responsible for the security of all school information accessed by that device. The member of staff should ensure:

- The device is password protected to an adequate level
- School work/emails are only accessible by them
- The device is secured and protected through industry standard methods
- Any potential data breach or theft of equipment is reported to the school data protection link officer and IT service provider within 24 hours
- Any school advice in relation to data management, security and protection is implemented

I declare the following:

- I understand that abuse of the network computers, printers, internet and any school device will not be tolerated. Abuse will result in my account privileges being suspended or revoked, and could lead to disciplinary action.
- I understand that the equipment is to be used primarily for school business and private use shall be ancillary and not significant otherwise tax liabilities may be incurred.
- I will use the schools equipment and facilities primarily for business use, and for personal use only with explicit written permission from the head teacher.
- I will only use school equipment to photograph and record students, and students' work, and in order to enhance professional activities.
- I will ensure I seek the relevant permissions prior to taking photographs of students and their work.
- I will protect my personal information on social media, and will comply with the school's social media guidance.
- I will use only those facilities I am authorised to use.
- I understand that my usage of these facilities may be monitored in accordance with telecommunications (lawful Business Practice – Interception of Communications Ref. 2000)
- I understand this declaration applies to all other mediums and equipment provided to me by Make It Different Trust.
- I am personally responsible for accessing school work/emails on my personal device(s) and I will ensure that all information is protected and kept secure

I confirm that I have read and understand the requirements of the school as set out in this declaration, and confirm I will adhere to these guidelines.

Name (in print) _____

Signed _____ Date _____