FALINGE PARK HIGH SCHOOL

CREATING COMPELLING LEARNING

E-SAFETY AND STAFF ACCEPTABLE USE POLICY

Date: September 2022

EQUITY
COMMUNITY
COMMUNICATION
DIVERSITY

Document Control:

Organisation	Falinge Park High School
Title	e-Safety and Staff Acceptable Use Policy
Author	IT Strategy Group
Filename	FPHS e-Safety and Staff AUP 2022
Owner	IT Strategy Group (S Ward – Deputy Head Teacher)
Subject	e-Safety
Review Date	June 2023

Revision History:

Revision Date	Reviser	Previous Version	Description of Revision
01 July 2022	S Ward	September 2021	Annual

Document Approvals – This document requires the following approvals:

Approval Sought From	Name	Date
Governors		TBC

Document Distribution – This document will be distributed to:

Individual/Group	Job Title/Group Type	Distribution Date
All Staff	All Job Titles	02/09/2022

CONTENTS

Whole school approach to the safe use of IT

Creating a safe IT learning environment includes three main elements at this school:

- an effective range of technological tools
- policies and procedures, with clear roles and responsibilities
- a comprehensive e-Safety education program for pupils, staff and parents

Roles and Responsibilities

E-Safety is recognised as an essential aspect of strategic leadership in this school and the Head, with the support of Governors, aims to embed safe practices into the culture of the school. The Headteacher ensures that the Policy is implemented and compliance with the Policy monitoring. The responsibility for e-Safety has been designated to a member of the senior management team – Mr S. Ward.

Our school e-Safety Co-ordinator is Mr S. Ward. The school's e-Safety coordinator ensures the Headteacher, Senior Management and Governors are updated as necessary. Our Designated Safeguarding Lead Mrs Julia Turrell and Safeguarding officers Mrs K Broadhurst and Mrs C Heywood support this work in school.

Governors need to have an overview understanding of e-Safety issues and strategies at this school. Governors will also be involved in the review of our e- Safety practices including areas such as filtering and other mechanisms for keeping our students safe. We ensure our governors are aware of our local and national guidance on e-Safety and are updated at least annually on policy developments. Training will be provided by the school where appropriate.

All teachers are responsible for promoting and supporting safe behaviours in their classrooms and following school e-Safety procedures. Central to this is fostering a 'No Blame' culture so pupils feel able to report any bullying, abuse or inappropriate materials. All members of the school community have a collective responsibility for e-Safety in the capacity appropriate to their role in school.

All staff should read, understand and implement the school's Policy relating to in-school and out of school practice, including:

- safe use of email
- safe use of the Internet including use of internet-based communication services, such as instant messaging and social networks
- safe use of school network, equipment and data including the use of data storage devices
- safe use of digital images and digital technologies, such as mobile phones and digital cameras
- publication of pupil information/photographs and the use of these on websites;
- e-Bullying/Cyberbullying procedures
- their role in providing e-Safety education for pupils
- their conduct under the 'Prevent' agenda

Staff are updated about e-Safety matters at least once a year/undertake annual training. This is built into the annual safeguarding training schedule that takes place.

1. Summary

This Policy document is drawn up to protect all parties – the pupils, 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. For the purpose of this policy, all teaching and support staff may be referred to as “staff” or “users” in terms of our school IT systems.

The school is committed to delivering compelling learning and therefore must provide an ICT system that enables this to take place when remaining secure and safe for all users. Staff must ensure they have read and understand this complete policy and related documents and will acknowledge this through the Google Form provided by leadership. Only staff who have accepted the terms will be permitted to use the ICT systems in school.

The e-Safety and Acceptable Use Policy for pupils is in the pupil planner and must be followed by pupils throughout the academic year. This outlines the expectations and sanctions imposed for misuse of school IT systems. A reference copy is available on the school website and pupils will receive and save an updated electronic copy of this annually. Failure to follow the standards and expectations set out by the agreement may result in pupil access being restricted.

All new Y7 pupils and parents will have this shared with them either physically or via an online form enabling them to acknowledge that they have received and understood the expectations. For all other year groups when significant changes to the policy have been made during the annual review this will also be further communicated. The designated ICT teacher will be responsible for ensuring that all pupils download and store the updated policy in their first ICT lesson.

Although the policy provides an extensive series of guidance and expectations you can seek further information regarding e-Safety through the school website by clicking on the “safeguarding at FPHS” tab and scrolling to the bottom of the page.

2. Context

This document provides a framework to protect all users, plus the school’s IT services and all data from all threats whether internal, external, deliberate or accidental. This includes all computing devices that can be connected to the network.

It is the policy of the school to ensure that:

- all computer systems, and information contained within them will be protected against unauthorised access
- information kept in these systems is managed securely, not only to comply with relevant Data Protection Legislation including GDPR, but also in a professional and dependable manner
- all members of staff are aware that it is their responsibility to adhere to this policy and adopt safe practice for any content they post, create or share online

- all breaches of ICT security are reported and subsequently investigated to minimise risk to pupils, staff, data and systems.

3. E-Safety

Guidance contained in KCSiE underpins all activity in school. Staff should be aware of online safety guidance therein.

- Staff should ensure that they are aware of e-safety issues affecting staff and learners. It is expected that staff complete regular e-safety training provided by the school and read and adhere to advice given by the School's IT Support Team.
- Staff should regularly remind learners of key e-safety messages and should model good e-safety practices.
- Staff must report any accidental access to inappropriate material to a member of the safeguarding team.
- Staff must report any inappropriate websites that are accessible to themselves or learners to a member of the safeguarding team.
- Staff should be vigilant when asking learners to search for images.
- If a learner accesses inappropriate material staff must report the incident to the safeguarding lead/officer and the IT Support Team.
- If staff suspect a child protection issue they must report it to their Designated Safeguarding Lead, following the correct procedures, including logging on My Concern.
- Staff must not pretend to be anyone or anything that they are not on the internet.
- Staff must report any suspicious emails or phishing attempts to the IT Support Team and inform them of any links that have been clicked upon.
- Staff must only communicate electronically with learners using their school provided email address and their own school account.

4. Computer Security

- Staff must use computers with care and leave ICT equipment as they found it.
- If it is noticed that ICT equipment or software is damaged or not working correctly, staff must report the issue to the IT Support team at the first opportunity.
- Staff must never try to bypass security features or systems in place on the network, or try to access resources or a user account that they do not have permission for.
- Staff must not attempt to install software on school computers or mobile devices unless they have permission from the IT Support Team. Any software changes or installations must be requested via the IT Support Team.
- Staff must always keep their user account credentials secure and not share them with anyone else.
- Staff are expected to recognise that their staff logon gives them access to systems and information that learners and other staff are not entitled to access and must not,

under any circumstances, allow anyone else access to a computer under their logon credentials (with the exception of the IT Support Team to resolve an issue reported by that member of staff).

- Staff must not attempt to go beyond their authorised access. This includes attempting to log on as another person, sending email whilst pretending to be another person or accessing another person's files. If staff find that they do have access to an area that they know they should not have access to, they must inform IT support personnel immediately.
- If a member of staff thinks that someone else has obtained their login details, they must report it to ICT support personnel as soon as possible in order for their password to be changed.
- Staff must never knowingly bring a computer virus, spyware or malware into school.
- If staff suspect a school computer or a removable storage device that they are using contains a virus, spyware or other malware, they must report this to ICT support personnel.
- Staff must not attempt to connect to another user's laptop or device while at school.
- Staff are not permitted to establish their own computer network.
- Staff must not reply to spam emails as this will result in more spam. Delete all spam emails.
- If any portable ICT equipment is lost or misplaced, staff must inform ICT support team immediately.

5. Physical Security and Management of IT Assets

Users should adopt safe practices by locking their user account if leaving their workspace, even temporarily. When not in use, all computer rooms or lapsafes should be locked to prevent unauthorised use or potential theft.

Users should report the following concerns to the IT Support team for further investigation:

- any suspicious use of the computer systems
- any accidental or malicious damage to ICT equipment
- any ICT equipment that is a hazard or looks unsafe
- any equipment that is malfunctioning
- reallocations of IT equipment without prior knowledge or consent

N/B

- Devices issued to staff remain property of the school. Upon your employment with the school ending, all IT related equipment should be returned to IT Support at your earliest convenience
- Any loss or damage to equipment discovered should be reported to IT Support without delay. Loss or damage costs may be charged to departmental budgets.

6. File Management

All users are responsible for managing files they create in any part of the network. This includes archiving or deleting files that are obsolete or out of date. Images which include pupils should not be removed from the network unless this is directly related to teaching and learning. Staff should take precautions to limit distribution beyond intended users. Images should not be stored in any school network or cloud-based storage areas accessed by pupils. For a more comprehensive explanation of your responsibilities, please see the Data protection and information policy accessible through the website.

7. Social Media

Digital Social Media is becoming increasingly a part of everyday life. All staff are reminded about the expectations from the Teachers' and Associates' Standards below. Use of social media is a safeguarding issue and as such its appropriate use is a non-negotiable at Falinge Park High school

All teachers and associate staff are expected to demonstrate consistently high standards of personal and professional conduct. The following statements define the behaviour and attitudes which set the required standard for conduct and can be related to the use of social networks.

All staff employed within school uphold public trust in the profession and maintain high standards of ethics and behaviour, within and outside school, by:	
i.	treating pupils with dignity, building relationship rooted in mutual respect, and at all times observing proper boundaries appropriate to a teacher's and associate staff members' professional position
ii.	having regard for the need to safeguard pupils' well-being, in accordance with statutory provisions
iii.	showing tolerance of and respect for the rights of others
iv.	not undermining fundamental British values, including democracy, the rule of law, individual liberty and mutual respect, and tolerance of those with different faiths and beliefs
v.	ensuring that personal beliefs are not expressed in ways which exploit pupils' vulnerability or might lead them to break the law

For further guidance relating specifically to Social Media all staff are expected to refer and adhere to the school Social Media policy accessible through the website.

The school has adopted the local authority's policy; Guidance on the use of Social Networking.

Part of this Policy headed Online contact with Children and Young People states:-

"As indicated within the safe working practice guidance document at Section 12.

"Social Contact", and Section 13, "Communication with pupils using Technology", it is inappropriate and totally unacceptable for staff to communicate via social networking sites with pupils and ex pupils. As stated within Section 4, "Duty of Care", staff have a duty to safeguard children and young people and must adhere to the schools safer working practice guidance in all of their actions, including online activities."

It is the responsibility of all teachers and associate staff to adhere to this e-Safety and Acceptable Use policy. They must ensure that they have read and fully understood it, seeking clarification where required.

8. Anti-Virus

It is the responsibility of all users to ensure that mobile school devices provided by the school are connected to the school network at least weekly in order to ensure antivirus software updates are applied. Any user who suspects a virus infection may exist on any school device must bring this to the immediate attention of the ICT support team.

9. Internet and Email Filtering

All internet access is subject to school's approved filtering systems. Some useful internet sites may be restricted. In these circumstances, users should contact IT support team to submit a request for access. In order to do this you must place a request on IT help desk following the process identified in the staff handbook. The IT team will endeavour to process the request in a timely fashion. Staff must take reasonable care and responsibility for searches conducted as part of teaching and learning. Content which causes concern should be reported immediately to the attention of the IT support team using the helpdesk system. Staff should also be aware that the use of the school internet access or systems (including email) to offer, provide or purchase products or services is forbidden without prior consent from Mr S Ward or Mrs J Richmond.

All school related emails must be sent out using the approved school email system. Under no circumstances should personal e-mail accounts be used for school business. Access to personal email accounts must be restricted to appropriate times e.g. lunchtimes and non-contact time. Users should be aware that all personal email activity is subjected to the same rigorous monitoring as for school email when using school IT services.

10. Copyright

The law of copyright applies to all electronic communication in the same way as it does to printed material and other forms of communication.

Users must ensure that files or software do not infringe copyright. Where this is found to be the case, they will be removed immediately.

Please see this link for further information https://copyrightandschools.org/dfe-agreements/

11. Monitoring

All computer activity is monitored and data may be accessed, intercepted and/or investigated as appropriate as part of the school's safeguarding procedures.

This is intended to ensure:

- that the security of school equipment and systems are not compromised
- information retrieval is possible when a user is absent (e.g. due to sickness)
- crime can be detected and prevented
- there is no unauthorised use of the IT systems
- the school implements and supports the 'Prevent' agenda
- all data that is held and processed in compliance within GDPR legislation and guidelines

When using email and the internet, users should:

- be aware that email is not a secure form of communication and users should be cautious about sending information of a confidential nature
- note that email is not suitable for the communications of confidential, personal or other sensitive information like comments relating to job performance or disciplinary issues, child safety or welfare matters
- be aware that email cannot be regarded as purely private, only to be seen by the receiver
- be mindful that the use of email should be treated with the same degree of care and professionalism as a typed letter and apply appropriate email etiquette
- not send email messages in the heat of the moment and avoid writing anything that may be construed as defamatory, discriminatory, derogatory, rude or offensive
- send email messages only to those whom the information is entirely relevant and necessary in the course of their work
- consider typing "secure" into the subject box of the e-mail as a prefix to encrypt the subsequent e-mail
- avoid sending large attachments and use alternative systems for sharing information if this is more efficient (eg. Google drive)
- take care when opening any email attachments, especially those from unknown senders or from computers from which virus protection may not be current or activated
- be aware that pornographic material is widely available on the internet and agree not, in any circumstances, to access, view, download or display any material that constitutes pornography or which is sexually explicit, politically sensitive, criminal information, sexist, racist, extreme or offensive in any other way. This will extend to sending any such materials by email or email attachment to anyone
- report to the safeguarding team if they accidentally access a website they consider to be pornographic or offensive or receive such material via the ICT systems. The offending material can then be deleted from the computer immediately and a record kept of the incident

- note that the deliberate act of accessing, viewing, uploading, downloading or displaying of such material will constitute gross misconduct
- be aware of the school's duty to protect copyright and not act in a way that will breach copyright or intellectual property rights
- be aware that the school may track the history of the internet sites they have visited and check email content

Users should note that this guidance will apply to any IT based communication, be it through web services, chat room, news groups or peer to peer sharing etc.

If you believe that you have received a file that may contain explicit material do not open it <u>in any circumstances</u> and report the matter to your school's Designated Safeguarding Lead or a member of the safeguarding team. You may be committing an offence if you knowingly access such a file even if investigating as part of your professional role.

12. Approved Software and Portable Devices

The school has a legal and financial requirement to ensure that all software installed on the computer system is legal. As such it is important that accurate records exist to comply with the law but to ensure the reliability and security of the computer system.

All portable storage devices like memory sticks are a convenient way of backing up your work and transferring it between different computers. However, use of such devices should be minimal with the use of Google Drive and desktop anywhere being preferable. Users should ensure that if they intend to use portable storage devices that they must work with the IT technical team to ensure that they are effectively encrypted and scanned for viruses as they will be personally liable for any data loss in line with GDPR expectations.

Please note where personal devices are configured for access into school systems and these are reported lost or stolen or on termination of employment, school reserves the right to return the device to factory settings. Where users are issued with any school owned devices, these must be returned to the IT support team on request in a timely fashion and in the condition that they were given out. Failure to do may result in further action by school leadership.

When using portable devices or considering software, users must:

- ensure that any devices or systems used to transfer information between work and home have up to date antivirus software
- not store confidential or personal information relating to any individual off site
- take reasonable steps to ensure that any computer equipment is stored securely and not at risk from theft
- be aware that if any device containing school data is lost or stolen, it must be reported to the school Data Protection Officer (Mr Simon Ward) and IT support, and staff should be prepared to list what data is at risk
- not install any software onto the school's equipment without obtaining permission from ICT support
- understand that any personal mobile device connected to the wired or wireless

network is subject to the same monitoring procedures as school devices

- not contact a parent or carer on any portable device other than their school work phone or another permitted device which has been agreed by the schools leadership team
- not contact pupils directly on their personal numbers unless this has been cleared with the Safeguarding Team and logged on MyConcern
- be aware that all new software purchases must go through IT Strategy group and be granted approval in order to be installed on school devices/systems. Any resources procured outside of the IT Strategy group cannot be used within school.

13. Cloud Computing

It is recognised that document storage can now be held virtually “in a cloud”. At Falinge Park High School this is possible by users uploading and storing information electronically making this accessible or shared online. Our school cloud-storage and communication system is based on Google Drive. No other cloud-based document sharing system should be used without approval from ICT Strategy Group. Users must be responsible for all documents they upload to any cloud-based system.

If staff require further clarification about the suitability of information they wish to upload to the cloud, they should refer to the school Data Protection Policy or seek advice from the school Data Protection Officer – Mr S Ward or Mr J Richmond.

If staff require further clarification about alternative cloud-based document sharing and communication systems they need to use within their school role, they should initially seek approval from the IT Strategy group.

14. Data Handling and Information Security

The school holds a variety of sensitive data including personal information about pupils and staff. If you have been given access to this information, you are reminded of your responsibilities under the revised Data Protection legislation (GDPR). Users must take appropriate steps to mitigate against data loss. For further advice, refer to the school Data Protection Officer – Mr S Ward or read further information in the data protection and information policy accessible through the school website.

When considering Data Handling and Security, users must:

- participate in a clear desk/clear screen policy to reduce the risk of unauthorized access, loss of and damage to information during and outside normal working hours or when areas are left unattended
- take reasonable steps to ensure that any electronic document/file containing confidential information is deleted from personal and shared network spaces once it is no longer required
- be aware that access to systems is restricted to those users who need it. Requests for access should be sought from the school Data Protection Officer (Mr S Ward)
- set strong passwords for user accounts and keep usernames and passwords

confidential. These must not be disclosed or shared with other users

- note that where information needs to be shared between organisations, secure networks must be used. It is never acceptable to transfer bulk personal information via normal email services. Further advice should be sought from the IT technical support team
- report promptly to the IT support team any incidents which may have security significance to the school

All users are advised to read fully the school's Information and Systems Security Policy. It is the responsibility of all users to adhere to this policy and ensure they have read and fully understood it.

15. Digital Images

There are no circumstances that justify adults working in a school possessing indecent images of children. Users who access and/or possess links to such material or websites will be viewed as a significant and potential threat to children. This will lead to criminal investigation and disciplinary action. Where indecent images of children are found and linked with a member of staff, the Headteacher must be informed immediately.

Indecent images should not be transferred from a pupil's phone to a personal device even in investigative purposes. In these circumstances, the safeguarding team must be consulted immediately.

Staff should only use approved school devices to take or store any photographs/video of children within a school setting. Under no circumstances should staff be expected or allowed to use their personal equipment to photograph/video pupils at or on behalf of the school. Requests for approved school devices must be made through the IT strategy group if an image or video is required.

Whilst images are regularly used for very positive purposes, staff need to be aware of the potential for these images to be taken and/or misused or manipulated for pornographic 'grooming' purposes. Particular regard needs to be given when images are taken of young or vulnerable children who may be unable to question why or how the activities are taking place. Pupils who have previously been abused in a manner that involved images may feel particularly threatened by the use of photography/filming. Staff should remain sensitive to any pupil who appears uncomfortable and should recognise the potential for misinterpretation.

There are no circumstances that justify any IT equipment belonging to the school being used to access any pornography; neither should any personal devices be used to access pornographic content whilst on school premises or remotely whilst using any school IT systems.

Users should take reasonable steps to ensure that pupils are not exposed to any inappropriate images/video content or web links. The school endeavors to ensure that internet filtering safeguards against this. Any unsuitable content accessed must be reported to a member of the senior team or IT technical staff immediately.

16. How will complaints regarding e-Safety be handled?

The school will take all reasonable precautions to ensure e-Safety. However, owing to the international scale and linked nature of Internet content, and the availability of mobile and SMART technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor Local Authority can accept liability for material accessed, or any consequences of Internet access.

Pupils

The **Compelling behaviour** policy must be enacted when IT infringements take place. This will involve the member of staff taking ownership for the recording and associated sanction. In cases of continued misuse/breach or incidents deemed to have a significant impact on teaching and learning or the safeguarding of pupils and staff, the member of staff is to report the incident to the head of year through the appropriate channels. This will then be escalated and addressed in line with the compelling behaviour policy

For pupils, infringements of this policy may result in one/a combination of the following sanctions:

- Senior detention, interview and/or counselling by Tutor/Head of Year/e-Safety Coordinator or Headteacher
- Re engaging and support understanding the breach related to e-Safety and/ or accessible use policy
- Informing parents or carers and potentially inviting them into school for further dialogue and support
- removal of internet or computer access for a period, (which could ultimately prevent access to files held on the system, including examination coursework)
- Period of time in reflection or fixed term suspension
- Referral to Local Authority and/or Police

Staff

Any concerns or complaints relating to staff misuse should be immediately reported to the Headteacher via the Headteacher's PA fittonl@falingepark.com.

Infringements of this policy will be investigated by a designated member of the senior leadership team (in most cases this will be the e-Safety coordinator) supported by the IT support team, where appropriate. This may lead to disciplinary action and in extreme cases could lead to dismissal under professional expectations and standards.