Contents

Introduction

This policy has been completed with reference to the comprehensive self-review tool, 360 degree safe.

This policy will be reviewed annually, or, if necessary, more frequently in response to any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place.

This e-safety policy has been developed by a working group made up of:

- Senior Leadership Team (including the Head teacher)
- E-Safety Coordinators
- School staff
- Governors
- Parents and Carers
- "e-Cadets" – the school's e-safety child-led initiative.

Consultation with the whole school community has taken place through a range of formal and informal meetings.

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity
- Surveys / questionnaires of
  - Pupils
  - Parents and carers
  - Staff

Scope of the Policy

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

The Education and Inspections Act 2006 empowers Head teachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the academy 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 academy, but is linked to membership of the academy. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The academy will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents and carers of incidents of inappropriate e-safety behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the e-safety roles and responsibilities of individuals and groups within the academy:

Governors:

The role of the E-Safety Governor will include regular meetings with the e-safety coordinators to monitor and discuss incident logs, incidents of cyber-bullying, and the provision of e-safety teaching in the school.

Head teacher:

- The Head teacher has a duty of care for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the E-Safety Co-ordinators.
- The Head teacher and (at least) another member of the Senior Leadership Team / Senior Management Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

E-Safety Coordinator(s):

- leads the e-safety committee
- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority / relevant body
- liaises with school technical staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- meets regularly with E-Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meeting / committee of Governors
- reports regularly to Senior Leadership Team

Network Manager:

The Network Manager is responsible for ensuring:

- that the academy’s technical infrastructure is secure and is not open to misuse or malicious attack
- that the academy meets required e-safety technical requirements and any Local Authority / other relevant body E-Safety Policy / Guidance that may apply.
- that staff users, and some older pupils, may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed. Younger pupils will be able to access a secure area of the network with a managed account.
- that the use of the network / internet / remote access / is logged and email is regularly monitored in order that any misuse / attempted misuse can be reported to the Head teacher; E-Safety Coordinators for investigation / action / sanction.

Teaching and Support Staff

are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current academy e-safety policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to the Head teacher or E-Safety Coordinator for investigation / action / sanction
- all digital communications with students / pupils / parents / carers should be on a professional level
- to closely monitor the use of any digital technology in the school and follow school policy with regard to their use.
- to ensure they are aware of the e-safety curriculum as taught at the Academy, thereby embedding e-safety as required into any lessons in which it may be relevant.

Safeguarding Designated Officer

should be trained in e-safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

E-Safety Group

The E-Safety Group provides a consultative group that has wide representation from the academy community, with responsibility for issues regarding e-safety and the monitoring the e-safety policy including the impact of initiatives.

Students / Pupils:

- are responsible for using the academy digital technology systems in accordance with the Pupil Acceptable Use Policy & Digital Rights Charter.

Parents / Carers

The academy will take every opportunity to help parents and carers understand the issues regarding the use of the internet & mobile devices through parents' evenings, newsletters, letters, the school website and information about national / local e-safety campaigns / literature. Parents and carers will be encouraged to support the academy in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website and on-line pupil records
- their children's personal devices in the academy (where this is allowed)

Community Users

Community Users who access school systems / website as part of the wider academy provision will be expected to sign a Community User AUP before being provided with access to school systems.

Policy Statements

Education – Students / Pupils

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across it. The e-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned e-safety curriculum should be provided as part of Computing / PHSCE and should be regularly revisited
- Key e-safety messages should be reinforced as part of a planned programme of assemblies (e.g. Safer Internet Day)
- Pupils should be helped to understand the need for the Pupil Acceptable Use Agreement & Digital Rights Charter and encouraged to adopt safe and responsible use both within and outside school.
- Any request from staff to make accessible sites that would otherwise normally be filtered should be auditable, with clear reasons for the need, and clear educational purpose.

Education & Training – Staff / Volunteers

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal e-safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the e-safety training needs of all staff will be carried out regularly.
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Agreements.
- The E-Safety Coordinator / Officer (or other nominated person) will receive regular updates through attendance at external training events
- The E-Safety Coordinator / Officer (or other nominated person) will provide advice / guidance / training to individuals as required.

Training – Governors

Governors should take part in e-safety training / awareness sessions, with particular importance for those who have responsibility for e-safety.

Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

- Academy technical systems will be managed in ways that ensure that the academy meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school academy technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to academy technical systems and devices
- All users (at KS2 and above) will be provided with a username and secure password by the Network Manager who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password. Pupils will be required to change their password on a termly basis. Staff will be required to change their password every 90 days.
- The "master / administrator" passwords for the academy ICT system, used by the Network Manager must also be available to the Head teacher and kept in a secure place (e.g. school safe)
- The Network Manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- Internet access is filtered for all users. There is a clear process in place to deal with requests for filtering changes.

- The school has provided enhanced / differentiated user-level filtering
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. The school infrastructure and individual workstations are protected by up to date virus software.
- Guests (e.g. trainee teachers, supply teachers) will be provided appropriate temporary access to school systems having read and agreed to the school Acceptable Use Agreement
- The Staff Acceptable Use Policy describes the extent of personal use that staff and their family members are allowed on school devices that may be used out of school.
- The Staff Acceptable Use Policy prevents staff from downloading executable files and installing programmes on school devices.
- The Staff Acceptable Use Policy describes the use of removable media (e.g. memory sticks / CDs / DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.
- The Staff Acceptable Use Policy describes the use of personal devices within the Academy.

Use of digital and video images

The school will inform and educate users about the risks associated with the use of digital and video images on the internet and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- The academy operates a policy whereby parents, carers and relatives of children at the school must not take photos of their children within the school, in order to safeguard privacy and in some cases the protection of all children.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

The academy will ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".
- It has a Data Protection Policy
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.
- The academy does not allow storage of personal data of any kind on memory sticks or any other removable media.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

	Staff & other adults				Students / Pupils				
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed		Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	X						X		
Use of mobile phones in lessons				X					X
Use of mobile phones in social time	X								X
Taking photos on personal phones / cameras				X				X	
Use of other personal mobile devices e.g. tablets, gaming devices		X							X
Use of personal email addresses in school, or on school network		X							X
Use of school email for personal emails				X					X
Use of messaging apps / platforms		X						X	
Use of social media		X						X	
Use of blogs		X						X	

Social Media - Protecting Professional Identity

The e-safety team should provide training in how to change security settings and how to stay safe on social media sites.

School staff should ensure that:

- No reference in personal profiles should be made in social media about pupils, parents or carers that could be interpreted in any way negatively, or that may compromise their personal information or safety.
- They should exercise extreme caution when engaging in online discussion on matters relating to members of the school community, to ensure that it is appropriate.
- Personal opinions should not be attributed to the academy or local authority.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

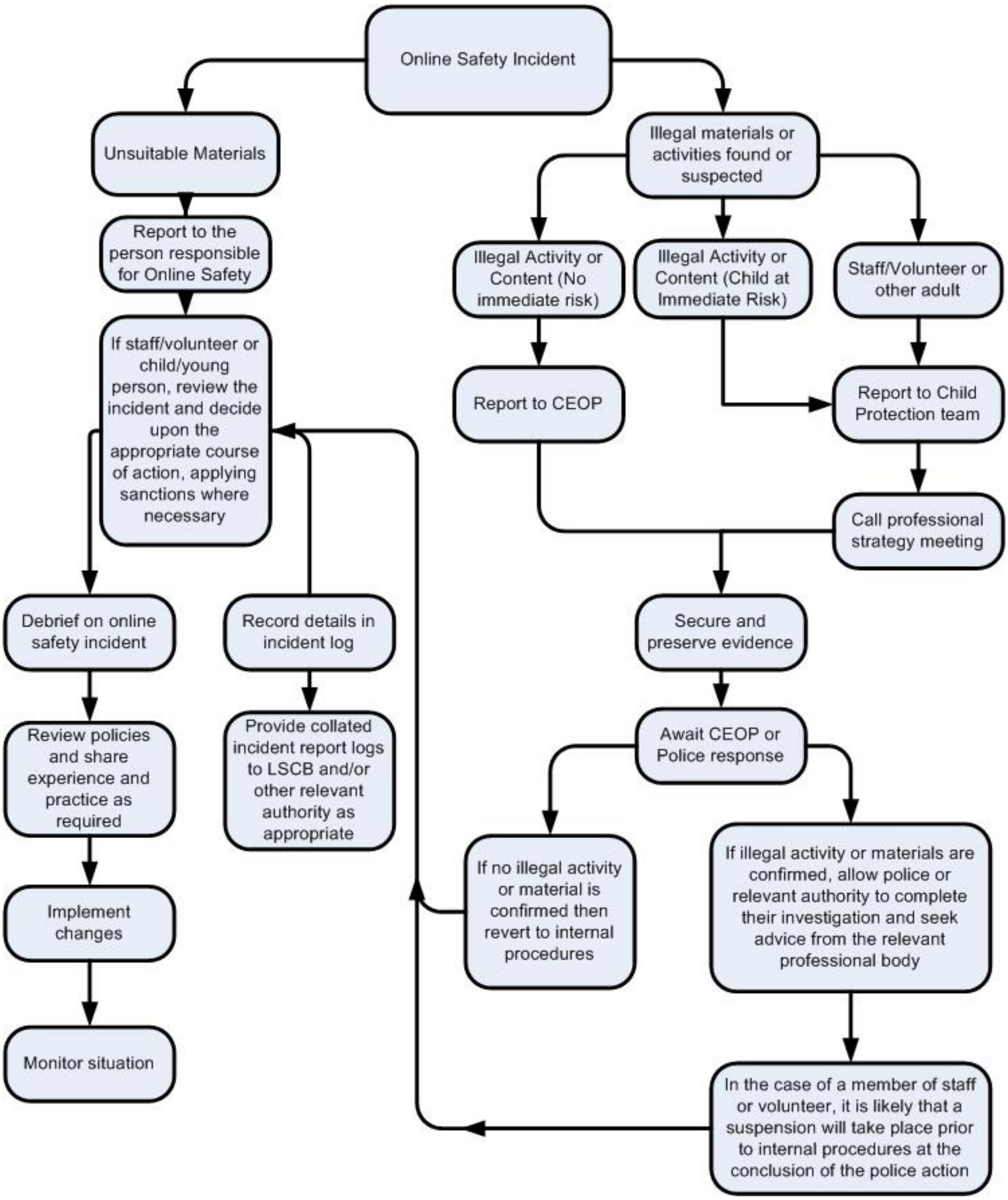
Unsuitable / inappropriate activities

School equipment or systems, and the use of equipment or systems while on school premises, shall only be used for professional purposes, including purposes that are for the educational benefit of the pupils at the school. Inappropriate or illegal use of equipment or systems would lead to possible disciplinary action.

Responding to incidents of misuse

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.


Online Safety Incident
Unsuitable Materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Review policies and share experience and practice as required
Implement changes
Monitor situation
Record details in incident log
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Illegal materials or activities found or suspected
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Secure and preserve evidence
Await CEOP or Police response
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow academy policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
  - Internal response or discipline procedures
  - Involvement by Local Authority or national / local organisation (as relevant).
  - Police involvement and/or action
- **If content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:**
  - incidents of 'grooming' behaviour
  - the sending of obscene materials to a child
  - adult material which potentially breaches the Obscene Publications Act
  - criminally racist material
  - other criminal conduct, activity or materials
- **Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.**

It is important that all of the above steps are taken as they will provide an evidence trail for the academy and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

Academy Actions & Sanctions

It is more likely that the academy will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour policies as follows:

Pupils	Actions / Sanctions								
Incidents:	Refer to class teacher / tutor	Refer to Head of Department / Head of Year / other	Refer to Head teacher / Principal	Refer to Police	Refer to technical support staff for action re filtering / security etc.	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction e.g. detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).			X	X					
Unauthorised use of non-educational sites during lessons	X							X	
Unauthorised use of mobile phone / digital camera / other mobile device	X							X	
Unauthorised use of social media / messaging apps / personal email	X							X	
Unauthorised downloading or uploading of files	X				X			X	
Allowing others to access academy network by sharing username and passwords	X				X			X	
Attempting to access or accessing the academy network, using another pupil's account	X				X			X	
Attempting to access or accessing the academy network, using the account of a member of staff	X		X		X				
Corrupting or destroying the data of other users	X		X		X				
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X		X		X	X			
Continued infringements of the above, following previous warnings or sanctions	X		X		X	X			
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X		X			X			
Using proxy sites or other means to subvert the school's / academy's filtering system	X		X		X				
Accidentally accessing offensive or pornographic material and failing to report the incident	X				X				
Deliberately accessing or trying to access offensive or pornographic material	X		X		X	X			
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	X				X				

Staff Actions / Sanctions

Incidents:	Refer to line manager	Refer to Head teacher Principal	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc.	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X	X			
Inappropriate personal use of the internet / social media / personal email	X	X			X			
Unauthorised downloading or uploading of files		X			X			
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	X				X			
Careless use of personal data e.g. holding or transferring data in an insecure manner	X				X			
Deliberate actions to breach data protection or network security rules		X	X		X		X	X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X	X	X	X		X	X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X	X	X	X		X	X
Using personal email / social networking / instant messaging / text messaging to carry out digital communications with students / pupils		X				X		
Communication which could compromise the staff member's professional standing		X				X		
Communication which could bring the school / academy into disrepute or breach the integrity of the ethos of the school / academy.		X				X		
Using proxy sites or other means to subvert the school's / academy's filtering system		X			X			
Accidentally accessing offensive or pornographic material and failing to report the incident		X			X	X		
Deliberately accessing or trying to access offensive or pornographic material		X	X		X		X	X
Breaching copyright or licensing regulations		X			X	X		
Continued infringements of the above, following previous warnings or sanctions		X	X		X		X	X

Acknowledgements

The Flying Bull Academy would like to acknowledge a range of individuals and organisations whose policies, documents, advice and guidance have contributed to the development of this E-Safety Policy.

- Members of the SWGfL E-Safety Group
- Avon and Somerset Police
- Representatives of SW Local Authorities
- Plymouth University Online Safety
- NEN / Regional Broadband Grids

October 2016