



# St Anne's School and Sixth Form College

## Online Safety Policy

Updated September 2018

### 1. INTRODUCTION

This policy document was written in conjunction with the Safeguarding of children and young people Policy at St. Anne's school and residence. Employees are responsible for following the standards of conduct laid down in this policy and should understand how this relates to the school ethos, safeguarding, anti-bullying Policies. At St Anne's School and Sixth Form College we believe that working in partnership with the East Riding of Yorkshire Local Authority, we have a duty to safeguard all pupils and students when using Information and Communication Technology (ICT). With the introduction of the Sixth Form, Online safety has never been as important.

The internet has become increasingly accessible for children and young people in places like schools, libraries and their own homes. Children and young people will experiment online, to enable them to take advantage of the many educational and social benefits of new technologies learners need opportunities to create, collaborate and explore in the digital world, using multiple devices from multiple locations (please see Mobile Devices Policy). However, all users need to be aware of the range of risks associated with the use of these internet technologies alongside the development of safe and responsible online behaviours.

### 2. RATIONALE

At St Anne's School and Sixth Form College and Residence we believe that working in partnership with the East Riding of Yorkshire Local Authority, we have a duty to safeguard all pupils and students when using information and communication technology (ICT).

This Policy document has been drawn up to protect all parties – the students, the staff, and the school and residence. The Policy provides clear advice and guidance on how to minimise risks and how to deal with any infringements.

### 3. AIMS

To provide a safe and secure environment for pupils and students to access ICT when in the school

and the residence.

To educate pupils and students on how to keep themselves safe when using ICT equipment at school, residence and at home.

To fulfil our school and residence's role to promote and support online safety.

## 4. KEY TASKS

### **Why Internet use is important at St Anne's School and Residence**

The Internet has become increasingly accessible for children and young people in places like schools, libraries and their own homes.

Children will experiment online at home, school and residence, to enable them to take advantage of the many educational and social benefits of new technologies.

Children need opportunities to create, collaborate and explore in the digital world, using multiple devices from multiple locations. However, all users need to be aware of the range of risks associated with the use of these internet technologies alongside the development of safe and responsible online behaviour.

### **How Internet use benefits children at St Anne's School and Residence**

A number of government projects have identified the benefits to be gained through the appropriate use of the Internet.

Benefits of using the Internet at St Anne's School and Sixth Form College and Residence include:

- \* access to experts in many fields for both pupils and staff;
- \* educational and cultural exchanges between pupils world-wide;
- \* access to world-wide educational resources including museums and art galleries;
- \* professional development for staff through access to national developments, educational materials and effective curriculum practice;
- \* collaboration across networks of schools, support services and professional associations;
- \* access to learning wherever and whenever convenient.

### **How we ensure Internet use enhances learning and life experiences at St Anne's School and Residence**

St Anne's School and Sixth Form College's Internet access will be designed to enhance and extend education. Children will be taught what Internet use is acceptable and what is not, and given clear guidelines for Internet use.

Staff at St Anne's School and Sixth Form College will ensure that the copying and subsequent use of Internet derived materials by staff and children complies with copyright law. Staff will guide children to online activities that will support the learning outcomes planned for their age, ability, additional

needs and maturity.

Children will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

### **How information systems security will be maintained at St Anne's School and Residence**

Security at St Anne's School and Sixth Form College is a major responsibility that includes not only the delivery of essential learning services but also the personal safety of staff, children and young people. The named person in charge of Data Security at St Anne's School and Sixth Form College is Mrs Lesley Davis.

All staff at St Anne's School and Sixth Form College with access to personal data understands that they are liable in law to protect that data. Should data be lost from an unencrypted USB drive or seen on a laptop used by other people, staff understand that the consequences could be serious for the member of staff and for the school. Staff use encrypted memory sticks to transport any such data between home/school.

Access to all ICT systems within the school and laptops that are taken home can only be accessed by a unique login and password for the individual (staff and small pupil cohort). Other pupils use a generic login and password.

All requests for access beyond that normally allocated (e.g. teachers wishing to access pupil personal storage) are authorised by the person in charge of data security. This includes the authorisation of access required by the ICT Support Team, theonepoint.

Where 'restricted' information is stored in SIMS or the server, access is only granted to individuals approved by the person in charge of data security, Mrs Lesley Davis.

Workstations are secured against user mistakes that compromise access or security and deliberate actions - Lock screen is used.

Servers are located in the HR room. Virus protection from Sophos for the whole network is installed and current. Access by wireless devices is pro-actively managed and is password protected.

### **How filtering is managed at St Anne's School and Residence**

Levels of Internet access are consistent across the school for children and staff separately, and access profiles are to a level appropriate for all members of the organisation.

St Anne's School and Sixth Form College uses theonepoint to manage the filtering systems within the school and ensure that systems to protect children and young people are reviewed and improved regularly. Broadband access includes filtering appropriate to the age and maturity of children.

Regular requests for filtering changes from within the organisation are made via Mrs Sara Tharratt, Schools' Business Manager, and Mrs Kay O'Neill (Residence). Mrs Sara Tharratt also ensures that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

### **How videoconferencing is managed at St Anne's School and Residence**

Video conferencing is a new emerging technology to be explored at St Anne's School and Sixth Form College. All videoconferencing equipment will be switched off when not in use and not set to auto answer. Videoconferencing contact information will not be put on the school Website. Videoconferencing will always be adult supervised.

Unique log on and password details for the videoconferencing services will only be issued to members of staff and kept secure.

All children will be reminded before video conferencing commences that they must not disclose their surname or other personal details.

Parent/Carers permission will not be required for video conferencing as permission is given on the school admission form.

All laptops with built-in web cameras should be covered (with a sticker or piece of card) when the laptop is in normal use to protect staff and students from videos of them being viewed by hackers.

### **How personal data is protected at St Anne's School and Residence**

The quantity and variety of data held on children, families and on staff is expanding quickly. While this data can be very useful in improving services, data could be mishandled, stolen or misused. St Anne's School and Sixth Form College fully complies with The Data Protection Act 1998, is General Data Protection Regulation compliant and is a member of the Information Commissioner Office website. Mrs Sara Tharratt, School Business Manager and Mrs Kay O'Neill, Residence Manager attend any Data Protection and Copyright Local Authority meetings as necessary (SIMS, GDPR etc).

When un-encrypted devices (cameras/iPads) are taken off site, all previous images will be deleted/stored on the server/encrypted memory stick, and then deleted off the device before leaving the school/residence grounds.

### **Password Security at St Anne's School and Residence**

All staff and some children at St Anne's School and Sixth Form College understand the importance of keeping their passwords secure from others. St Anne's School and Sixth Form College recommends to all staff to use a different password for accessing organisational systems to that used for personal (non-organisational) purposes. When leaving a computer for any length of time, all staff members/volunteers are told to log off or lock the computer, using CTRL+ATL+DELETE.

### **How email is managed at St Anne's School and Residence**

Staff are provided with a school email address that they can use if they feel it is appropriate. Email management is the responsibility of Mrs Kay O'Neill (Residence Manager) and Mrs Debbie Johnson (Administration).

### **How published content is managed at St Anne's School and Residence**

The contact details on the website are the main address, email and telephone number for the school. No other personal contact information will be published, including the use of children's full names. Mrs Kay O'Neill (Residence Manager) takes overall editorial responsibility and ensures that

content is accurate and appropriate. Parents/Carers are given regular reminders on the weekly Parentmail about appropriate content on the website. The website complies with all guidelines for publications including respect for intellectual property rights and copyright.

### **How the St Anne's Twitter account is managed at St Anne's School and Residence**

Information is put on the school Twitter feed only by Kay O'Neill, Sharron O'Keefe or Rachel Pearson using a specific staff-only iPad or via a staff log-in on a school computer. Only photos of students who have parental permission for their photos to be used on social media are included on the St Anne's Twitter page and it is the teacher's responsibility who is requesting the posting to check that students who are shown on Twitter have the correct permissions to be photographed. Full names are not used and should not be visible on students' work or in the background of photos. Photos are always taken on class iPads or cameras as photos on personal devices is contradictory to our Online Safety Policy. Photos should be emailed to lead staff from school email addresses only.

Students should be made aware of Twitter and how they can use it safely as even though they cannot directly tweet (using the school Twitter account) but should know how to keep themselves safe. Parents and staff can follow our Twitter page, but will not be followed back.

### **How social networking and personal publishing is managed at St Anne's School and Residence**

All adults have been made aware of the potential risks of using social networking sites or personal publishing, either professionally with children and young people or personally. They have been made aware of the importance of considering the material they post, ensuring profiles are secured and how publishing unsuitable material may affect their professional status. All staff have read and understood the professional standards and guidance about using these social media technologies. All staff know that all communications with pupil/parents/carers should be made through official school systems.

Pupils who do use social networking have been advised not to publish specific and detailed images or private thoughts, especially those that may be considered threatening, hurtful or defamatory when using the Internet at school or home.

### **How Internet access is authorised**

St Anne's School and Sixth Form College maintains a current record of all staff/volunteers and children who are granted access to the organisation's electronic communications.

All staff/volunteers read and sign the organisation's policies regarding information security and the use of information technology before using the organisation's ICT resources. For younger children, access to the Internet is by adult demonstration with occasional directly supervised access to specific, approved on-line materials. Every child and adult in the school and residence will agree to comply with and sign the Acceptable Use Policy (parents can sign for the child if necessary).

Parents/Carers will be informed that children and young people will be provided with supervised and unsupervised Internet access, but must comply with the Acceptable Use Policy at all times.

### **How risks will be assessed at St Anne's School and Residence**

St Anne's School and Sixth Form College will take all reasonable precautions to ensure that users

access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a computer. Neither St Anne's School nor ERYC can accept liability for the material accessed, or any consequences resulting from Internet use.

St Anne's School will audit digital technological use to establish if the Online Safety Policy is adequate and that the implementation of the Online Safety Policy is appropriate. The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

Methods to identify, assess and minimise risks will be reviewed regularly.

### **How complaints will be handled at St Anne's School and Residence**

Parents and staff know how to use St Anne's School and Sixth Form College complaints procedure. Children know they can speak to any member of staff across the school and residence. Potential child protection and illegal issues will be referred to the Child Protection coordinator Mrs Kay O'Neill and Online Safety coordinator, Mrs Lesley Davis.

The 'Response to Risk Flowchart' for reporting online safety incidents will be followed by the school and residence staff, and the incident log sheets will be filled out accordingly. Any complaint about staff misuse will be referred to the Online Safety coordinator, Mrs Lesley Davis. All Online Safety complaints will be recorded by Mrs Lesley Davis — including any actions taken. Children and parents will work in partnership with St Anne's School and Sixth Form College to resolve any issues.

### **How the Internet and online safety will be used across the community**

The school will liaise with local organisation's (including East Riding of Yorkshire Council) to establish a common approach to online safety. The Online Safety lead, Sharron O'Keefe will attend any online safety related courses to remain up-to-date with any developments.

The school will be sensitive to Internet related issues experienced by children and young people out of school, e.g., social networking sites, online gaming and offer appropriate advice when needed.

### **How Cyber bullying will be managed at St Anne's School and Residence**

Cyber bullying (along with all forms of bullying) will not be tolerated at St Anne's School and Sixth Form College. Full details are set out in St Anne's School' policy on anti-bullying. There are clear procedures in place to support anyone affected by cyber bullying. All incidents of cyber bullying are reported to Mrs Lesley Davis and/or Mrs Kay O'Neill, Residence Manager and will be recorded.

See section 5. Sanctions

### **How St Anne's School and Residence responds to an Incident of Concern**

An important element of online safeguarding at St Anne's School and Sixth Form College is the ability to identify and deal with incidents of concern and those related to the confidentiality of information.

All staff/volunteers and children know that they have a responsibility to report online safety or online security incidents so that they may be dealt with effectively and in a timely manner in order to

minimise any adverse impact. St Anne's School and Sixth Form College and residence has an incident reporting procedure and records reported incidents in an Incident Log.

The Incident Log will be kept by Mrs Lesley Davis and will be reviewed termly by the Governing Body – Mr Geoff Ogden (Safeguarding and Online Safety Governor)

The children and staff at St Anne's School and Sixth Form College understand and know how to use the 'Hector Dolphin' internet safety button and how to make an iPad 'safe'.

### **How Communication is handled at St Anne's School and Sixth Form College and Residence**

St Anne's School and Sixth Form College will include appropriate communication and training for all people (children and adults alike).

This will cover:

- \* Workforce training in understanding the rationale for all online safeguarding procedures and the consequences of inappropriate practice.
- \* Workforce training in responsible approaches to data on mobile devices, communicating online and procedures when using multimedia digital content such as photographs, videos and podcasts in terms of permission seeking, taking, storage and retention.
- \* A comprehensive and developmental online safety curriculum for children including the responsible use of web and communication technologies both inside and outside school (Residence) and risks related to cyber bullying.
- \* Annually re-visiting of the AUP with staff and pupils.
- \* Ensuring non-teaching staff are trained and up-to-date in their subject knowledge
- \* Up-to-date Acceptable Use Policies (AUPs) based on all the agreed procedures for online security and online safety and covering ICT usage by all sectors of the organisational community. This policy shall be subject to annual review by the governing body.

### **How this policy will be introduced to children at St Anne's School and Residence**

A copy of the online safety policy has been attached to the acceptable use policy for all staff and parents to be aware of its contents and discuss with children how they feel it is appropriate. Online safety will feature regularly for discussion at termly minutes for The Computer Safety Group.

The school as a whole regularly teaches online safety as part of dedicated and discreet ICT online safety lessons. The 'Think You Know' documents have been used by every class across the school and residence. Before children access the Internet, safe and responsible use of the internet and technology is reinforced.

### **How the policy has been discussed with staff at St Anne's School and Residence**

The Online Safety Policy has been formally provided to and discussed with all members of staff. To protect all staff and children, St Anne's School and Sixth Form College has implemented Acceptable Use Policies, which are to be signed every year by all staff, children, volunteers and parents.

Staff are aware that Internet traffic can be monitored and traced to the individual user - discretion and professional conduct is essential.

Theonepoint who manage the schools' filtering systems are regularly supervised by Mrs Sara Tharratt, the schools' Business Manager by means of setting a job sheet and prioritising work.

When staff are provided with digital devices (e.g. laptops) by St Anne's School that may be accessed outside of the organisational network, staff are clear about the safe and appropriate use of the provided equipment and rules about use of the equipment by third parties. Staff are aware of their responsibility to maintain confidentiality of the organisation's information.

All staff within St Anne's School and Sixth Form College, including administration staff and governors, are included in awareness raising and training. Induction of new staff/volunteers includes a discussion of the organisation's Online Safety Policy.

### **How parents/Carers support will be enlisted**

Internet use in children's homes is increasing rapidly, encouraged by low cost access and developments in mobile technology. Unless Parents/Carers are aware of the dangers, children and young people may have unrestricted and unsupervised access to the Internet in the home.

The school will help parents/Carers plan appropriate supervised use of the Internet at home and will educate them on the risks by providing an 'Online safety Parents' Awareness Evening' or information to send home, with follow-up information for those unable to attend.

Parents'/Carers attention has been drawn to St Anne's School Online Safety Policy by providing them with a copy of this policy annually, along with a copy of the appropriate Acceptable Use Policies.

## **5.SANCTIONS AND DISCIPLINARY PROCEEDINGS**

Sanctions and disciplinary procedures will be taken where users visit internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

- pornography, adult or mature content
- promotion of any kind of discrimination, racial or religious hatred
- information regarding terrorism or going against the Prevent strategy
- personal gambling or betting
- personal use of auction sites
- any site engaging in or encouraging illegal activity
- threatening behaviour, including promotion of physical violence or mental harm
- any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute
- using school systems to run a private business
- use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by SWGfL and the school



- revealing or publicising confidential or proprietary information (e.g. financial or personal information, databases, computer or network access codes and passwords)
- creating or propagating computer viruses or other harmful files
- carrying out sustained or instantaneous high volume network traffic (downloading or uploading files) that causes network congestion and hinders others in their use of the internet

### Sanctions for misuse: PUPILS

Incidents:	Refer to class teacher/tutor/SCCO	Refer to Head Teacher/Childcare Manager	Refer to police	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	✓	✓	✓	✓	✓		✓
Unauthorised use of non-educational sites during lessons	✓	✓		✓		✓	
Unauthorised use of mobile phone / digital camera / other handheld device	✓	✓		✓		✓	
Unauthorised use of social networking / instant messaging / personal email	✓	✓		✓		✓	
Unauthorised downloading or uploading of files	✓	✓		✓		✓	
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	✓	✓		✓		✓	

### Sanctions/Actions: STAFF

Incidents:	Refer to Head teacher/Childcare Manager	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for	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).	✓	✓	✓		✓	✓	✓
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email	✓				✓		
Unauthorised downloading or uploading of files	✓				✓		
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	✓				✓		
Careless use of personal data e.g. holding or transferring data in an insecure manner	✓				✓		
Deliberate actions to breach data protection or network security rules	✓	✓			✓		
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	✓		✓				✓
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature to staff	✓	✓			✓		
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature to learners	✓	✓			✓	✓	✓
Breach of the school online safety	✓				✓		

policies in relation to communication with learners							
Using personal email / social networking / instant messaging / text messaging to carry out digital communications with pupils	✓				✓		
Actions which could compromise the staff member's professional standing	✓				✓		
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	✓				✓		
Accidentally accessing offensive or pornographic material and failing to report the incident	✓				✓		
Deliberately accessing or trying to access offensive or pornographic material	✓						✓
Breaching copyright or licensing regulations	✓				✓		
Continued infringements of the above, following previous warnings or sanctions	✓		In some cases				✓

## 6. REVIEW OF THE POLICY

A review of the policy will be undertaken in line with the policy review timetable and any amendments or updates will be reported to the Governing Body.

Any new legislation or directives will be incorporated into the policy as necessary.

Date: 23.09.18

Review Date: 23.09.19