

**RATIONALE**

This policy is one of a series in the Academy's integrated safeguarding portfolio. Our core safeguarding principles are:

the Academy's responsibility to safeguard and promote the welfare of students is of paramount importance

safer students make more successful learners

representatives of the whole-school community of students, parents, staff and governors will be involved in policy development and review

policies will be reviewed annually, unless an incident or new legislation or guidance suggests the need for an interim review.

Through our day-to-day contact with learners and families, all staff have a crucial role to play in noticing indicators of possible abuse or neglect and in referring concerns to the appropriate agency.

**Introduction**

**The first priority of Bradford Academy is safeguarding the wellbeing of our students. We are committed to the highest standards in protecting and safeguarding the students entrusted to our care at all times.**

Safeguarding is the process of protecting children from abuse or neglect, preventing impairment of their health and development, and ensuring they are growing up in circumstances consistent with the provision of safe and effective care that enables children to have optimum life chances and enter adulthood successfully.

**1. What is E-Safety?**

Whilst the Internet and associated technologies are an excellent tool and resource to enrich learning there are still dangers related to their use, especially in relation to young students. Some examples of this are:

Bullying via chat or email

Obsessive Internet use

Exposure to inappropriate materials

Inappropriate or illegal behaviour

Physical danger of sexual abuse

As a school it is our duty of care alongside that of parents and other members of the community to protect our children from these dangers and this can be achieved by many different mechanisms working together.

The purpose of this e-safety policy is to outline what measures Bradford Academy takes to ensure that students can work in an e-safe environment and that any e-safety issue is detected and dealt with in a timely and appropriate fashion.

We aim to use education of safe and responsible use as the key method for ensuring students remain safe whilst online. This will be backed up by the use of monitoring systems, procedures, accountability methods for dealing with issues.

## **2. Audience**

This document is intended for public consumption as well as that of Academy members, parents and local community and is a clear outward statement on the Academy e-safety practices.

## **3. General policy statement**

The Academy will endeavour to ensure the e-safety of all Academy members. It will use education, technology, accountability, responsibility and legislation as the key ways to achieve this.

## **4. Whole Academy responsibilities for e-safety**

Within the Academy all members of staff and students are responsible for e-safety. Responsibilities for each group include:

### **Students**

Participating in and gaining an understanding of e-safety issues and the safe responses from e-safety training sessions. To work in a safe and responsible way when using ICT facilities.

Compliance with a highly visible student's Acceptable Use Policy (AUP) which students must agree to each time they use Academy ICT equipment either in the Academy or remotely.

Reporting any e-safety issue to the teacher, team leader, ICT Support Team or parent.

Take responsibility for their own actions using ICT, the Internet and any other communications technologies.

### **Student Council**

Responsible for reviewing the student Acceptable Use Policy, making changes where necessary to cover changes in technology or changes in usage. The annual review to take place in conjunction with the Lead Practitioner for ICT and the Information Systems Director.

### **All Staff**

Have a clear understanding of e-safety issues and the required actions from e-safety training sessions. Reporting any e-safety issues to the Information Systems Director or a member of the ICT Support Team as soon as the issue is detected.

Compliance with the staff Acceptable Use Policy (AUP) at all times when they use Academy ICT equipment either in the Academy or remotely which connects to the Internet. This staff AUP also applies when accessing Academy systems from non-Academy equipment and staff should also follow this policy when using ICT at all times outside of the Academy to ensure their safety.

### **Teaching Staff**

Educating students on e-safety through specific e-safety training sessions and re-enforcing this training in the day to day use of ICT in the classroom.

### **Lead Practitioner for ICT**

Responsible for ensuring e-safety training is given to both staff and students at appropriate times. To ensure Acceptable Use Policies are signed by students in their Planners.

Responsible for ensuring an annual review of the Acceptable Use Policy is done with the Student Council or other representatives of the students.

Works with the Information Systems Director, Information Systems Manager and Student Council to create, review and advise on e-safety and acceptable use policies.

### **Information Systems Director**

Deals with e-safety breaches from reporting through to resolution in conjunction with the Support for Learning team.

Works with the Lead Practitioner for ICT, Information Systems Manager and Student Council to create, review and advise on e-safety and acceptable use policies.

Works with outside agencies including the police where appropriate.

To review ICT monitoring systems for both staff and student activity at regular intervals.

Maintains a log of all e-safety issues.

Works with the Governor responsible for Safeguarding to ensure that procedures and policies are robust and ensure that we are doing our utmost to help ensure our staff and students can work and learn in a safe and secure environment whilst ensuring access is unhindered in any way which would affect the standards of teaching and learning.

### **Lead Behaviour Professional**

To work with the Information Systems Director to agree actions and sanctions for breaches of the Student AUP. To ensure all e-Safety incidents are dealt with thoroughly by members of the Pastoral Team and the actions recorded by way of a Behaviour Incident Sheet where appropriate.

### **Information Systems Manager**

Ensure that the best technological solutions are in place to ensure e-safety whilst still enabling students to use the Internet and ICT systems effectively in their learning.

Ensure that all information captured using these systems is secure, accessible to the appropriate members of staff, and stored in a robust manner. In addition securing and preserving evidence of any e-safety breach.

Checks and audits of all systems to ensure that no inappropriate data is stored or is accessible.

Work with the Information Systems Director, Lead Practitioner for ICT and Student Council to create, review and advise on e-safety and acceptable use policies.

### **Designated Member of ICT Support Team**

To review ICT monitoring systems at intervals during the day. This monitoring is limited to student activity only. To report any breaches to the Information Systems Director and Pastoral Support Team where necessary. To begin the process of recording the event in the e-Safety Log.

### **Pastoral Team**

To report any breaches of the AUP to the Information Systems Director and Lead Behaviour Professional where necessary.

To deal with any issues flagged up by monitoring systems or any other method.

To impose sanctions as appropriate. Sanctions may include a punishment such as removal of access to Internet during free time, detention and where deemed necessary communications with parents or police.

To ensure that a Behaviour Incident Sheet is completed where deemed necessary.

### **e-Safety Team**

To meet on a regular basis to review procedures and policies

To meet at regular intervals to review latest breaches of the student AUP and e-Safety Incident Log.

To ensure that the roles, responsibilities and procedures within the this policy are carried out and reviewed when necessary.

## **5. How the Academy ensures e-safety in the classroom**

### **Educating students in e-safety**

A clear objective of the Academy is to educate students in safe use of ICT and the Internet. We feel this is the best way to minimise the potential for any e-safety issues to occur. This will also provide students with a good basis of knowledge on e-Safety which can be used outside of the Academy and in later life.

Students will receive specific e-safety lessons aimed at ensuring that:

Students know the e-safety risks that exists and how to identify when they are at risk.

Students know how to mitigate against e-safety risks by using e-safe practices whilst online.

Students know when, how and to whom to report instances when their e-safety may have been compromised.

Students know that they are in an environment that encourages them to report e-safety issues without risk of reprimand, humiliation or embarrassment.

The Academy will follow the Think U Know programme by the governments Child Exploitation and Online Protection (CEOP) centre as one of the primary education tools.

In addition to this specific training all members of staff will have a duty to reinforce e-safety practices wherever possible and will offer students advice and support in the classroom where minor e-safety incidents have occurred.

E-Safety education information will have high visibility in all areas of the Academy.

### **Acceptable Use Policies**

All Academy members both students, staff and parents must agree to an Acceptable Use Policy (AUP) before they can use Academy ICT systems. With respect to e-safety the AUP details:

The users responsibilities

Activities which are appropriate and inappropriate

Best practice guidelines

How the Academy will monitor e-safety

What information is collected

### **How e-safety is monitored**

The Support for learning department and IT Support Team will actively monitor the students ICT activity using monitoring systems which can flag potential e-safety issues.

The ICT Support Team will periodically review Internet access logs to track any websites which could potentially present an e-safety issue.

The Information Systems Director will periodically review the E-Safety log to track, trends and use the information to look at ways of improving the student's e-safety.

Teaching staff will directly monitor the students ICT and Internet use in the classroom. This is done by manually monitoring and also using IT tools available in the classroom.

### **How technology is used**

The Academy will employ many different technologies to help to ensure e-safety for all the Academy members;

The Academy will use Internet filtering to block inappropriate content as designated by the DCSF and BECTA and in addition block websites which are irrelevant to the student's programme of study and are considered time wasting.

The Academy will allow the use of some categories of site considered 'time wasting' during students' free time, such as at breaks, to promote appropriate use at appropriate times.

The Academy will use a system which tracks all student activity on the Academy's computers. This system will automatically flag potential e-safety issues which will be monitored and then can be investigated by the support for learning team.

The Academy will restrict which activities the students can perform using ICT and the Internet through systems security policy and access control.

Teaching staff will use control mechanisms to attempt to limit the applications and web sites which the students can visit whilst using ICT within a lesson.

## 6. How the Academy will respond to issues of misuse

The following are provided for the purpose of example only. *Whenever a student or staff member infringes the e-Safety Policy, the final decision on the level of sanction will be at the discretion of the Principal.*

### Students:

Breaking the rules within the AUP will be dealt with in the following ways (See Appendix i for AUP):

**Rules 1-8** will be dealt with in a similar way to classroom behaviour problems.

1. First a teacher would log the issue on ePortal using the Behavior System. An event/behavior type will be setup for 'ICT abuse' on CMIS.
2. The next step for continued rule breaking will be a departmental detention (break time or afterschool as the teacher sees necessary).
3. The final step then for continued rule breaking and where all other options do not work would be for Internet and/or email privileges to be withdrawn. This will be done through Phil Allen and requests for this will come through him to the IT Team and not directly from teaching staff.

**Rules 9 & 10** will immediately escalate to the Pastoral Team and will probably be dealt with by James our in-house Police officer depending on the severity. Sanctions which may be given to them:

- a bill for the cost of repair/replacement,
- some type of community service with a rate of pay attached so that any bill can be worked off,
- any other sanction our Police Officer deems appropriate.

We will try where possible to have our Police officer deal with these issues as a criminal offence. **We should also make it very clear to students that they will be dealt with in this way.**

### Staff:

#### Category A infringements (Misconduct)

Excessive use of Internet for personal activities not related to professional development e.g. online shopping, personal email, instant messaging etc.

Misuse of first level data security, e.g. wrongful use of passwords

Breaching copyright or license e.g. installing unlicensed software on network

*[Sanction - referred to line manager / Principal / Warning given.]*

#### Category B infringements (Gross Misconduct)

Serious misuse of, or deliberate damage to, any school computer hardware or software;

Any deliberate attempt to breach data protection or computer security rules;

Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent;

Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988;

Bringing the Academy into disrepute.

*[Sanction – referred to Principal and follow Academy disciplinary procedures / Police/ GTC/ Governors]*

**Child Pornography or any other issue relating to child protection:**

In the case of child pornography being found, the member of staff will be **immediately suspended** and the Academy disciplinary procedures implemented.

**Other safeguarding actions:**

Remove the PC to a secure place to ensure that there is no further access to the PC or laptop.

Instigate an audit of all ICT equipment to ensure there is no risk of pupils accessing inappropriate materials in the school.

Identify the precise details of the material.

Where appropriate, involve external agencies as part of these investigations.

**How will staff and students be informed of these procedures?**

Procedures are included within the school's e-safety / Acceptable Use Policy. All staff are required to sign the school's e-safety Policy acceptance form;

Pupils will be instructed about responsible and acceptable use and given strategies to develop 'safe behaviours'. Pupils are required to sign an age appropriate e-safety / acceptable use form.

**7. Working with parents and the community**

Clearly many Academy students will also have access to ICT and the Internet at home, often without some of the safeguards that are presents within the Academy environment. Therefore parents must often be extra vigilant about their child's e-safety at home.

One of the goals of the Academy is to support parent's role in providing an e-safe environment for their children to work in outside the Academy.

The Academy will do this in several ways;

Run training sessions and workshops on general ICT use and e-safety.

Publish e-safety information and direct parents to external e-safety advisories via the Academy online parents portal and Academy website.

**8. Acceptable Use Policies**

The Academy has the following acceptable use policies in place which must be agreed to before the relevant individuals will be able to access ICT systems and the Internet.

Staff ICT and the Internet Acceptable Use Policy

Students ICT and the Internet Acceptable Use Policy

A copy of these policies are available on request. The Academy will regularly review and update these policies.

## **Appendix i - Student AUP**

Keeping safe: stop, think, before you click!

10 rules for responsible ICT use

These rules will help keep everyone safe and help us to be fair to others.

You must accept these rules before you will be allowed to use the ICT facilities within Bradford Academy.

- 1. I will not look at other peoples files without their permission and will only delete my own files.**
- 2. I will only do schoolwork during lessons.**
- 3. I will keep my login and password secret.**
- 4. I will not keep inappropriate files on the school network or in my user account.**
- 5. No unnecessary emailing. This includes in and out of lessons.**
- 6. The messages I send and the things I upload will only be polite and sensible.**
- 7. I will only email people I know and/or my teacher has approved.**
- 8. If I am unhappy with a message received, I will not respond to it and report it to a member of staff.**
- 9. I will treat the ICT equipment with respect and will not cause damage to it.**
- 10. I will not download or upload anything which is offensive, illegal or is copyrighted.**

# Top Tips to keep your child safe

The safety of your child is really important to us, and we do everything we can to make sure that your child learns in a safe environment. You can find details of what we do in our Safeguarding Policies—you can read these on our website [www.bradfordacademy.co.uk](http://www.bradfordacademy.co.uk) or ask reception for copies. We have also put some advice in the student planner—please look at this, and talk to your child about it.

We all remember our teenage years and how difficult these can be (both for the teenager and the parent/carer!). However, sometimes, a change in behaviour could signal that something bad is happening to them. Instances of child abuse and bullying are rare, but sadly they do happen. Below are a list of things to look out for which may be signs of abuse or bullying.

## Child abuse and what to look for

It is important that you know what to look for in the event that a child is being abused—there are four types of abuse— physical, emotional, sexual and neglect. Most cases of abuse happen with someone the child or family knows rather than a stranger.

If the unthinkable happens, you may notice:

- bruises or other injuries
- a change in behaviour – from quiet to loud, or from happy-go-lucky to withdrawn
- pain or discomfort
- fear of a particular person, or a reluctance to be alone with them
- secrecy around a relationship with a particular person
- reluctance to discuss where they go, or who they are with
- sexual talk or knowledge beyond their years
- being watchful, or always on edge
- losing interest in their appearance, hobbies or family life
- alcohol or drug taking
- having money and refusing to say where it has come from
- wetting the bed
- becoming clingy

## Signs of Bullying include:

- Reluctance to go to school, truancy, lateness
- Torn clothing, losing dinner money or asking for more money than usual
- Complaining of regular headaches or stomach aches
- Unexplained bumps or cuts

If you notice any of these things, try talking to your child; if you are not satisfied with their explanation (remember, they might be scared to admit what is happening), talk to our designated Child Protection Officers, who can give you advice and support.



John Craig

[j.craig@bradfordacademy.co.uk](mailto:j.craig@bradfordacademy.co.uk)

01274 256696

[s.reynolds@bradfordacademy.co.uk](mailto:s.reynolds@bradfordacademy.co.uk)

01274 2566849



Sandra Reynolds

# Top Tips to keep yourself safe

Your safety is really important to us. At the Academy, we do everything we can to make sure that you learn in a safe environment.

Sticking to the Academy Value Contract is one way that you can help us to do this. Below are a list of tips to help you to keep safe, both inside and outside of the Academy.

- Look confident. People are less likely to pick on you.
- Try to go places with friends. If you do go out alone always tell someone where you are going and what time you will return.
- Talk to a trusted adult – someone in the family or someone at school – if anyone says or does anything that worries or frightens you.
- Don't worry about breaking rules if you feel afraid. It's OK to shout at or run away from an adult who is trying to hurt you.
- Carry a mobile phone and put emergency numbers – your parents, police, a trusted adult – on speed dial so you can make a call quickly if you need to.
- If you are taking a bus or train, make sure you have enough money for the return journey. Don't accept money from someone you've never met before.
- Don't accept a lift from someone you've never met before. Call someone to pick you up.
- Stick to well-lit areas where there are people around if you need help.
- Remember that alcohol and drugs can harm your health and can also encourage you to take unnecessary risks.
- This may seem silly – but if someone is frightening you and you can't get away, pretend you are going to be sick over them. It makes them move back, giving you a chance to run.

**Remember, if an adult tries to hurt you it's not your fault. You don't have to do what they say just because they are an adult. Try to find the confidence to tell**



**Mr Craig**



**Mrs Revnolds**