Bradford Grammar School

E-Safety Policy

This policy applies to the Senior School and is published to parents, pupils and employees. Issued 1 March 2015

1. Introduction

The Designated Safeguarding Leads (DSLs), Deputy Head and Pastoral Director have overall responsibility for e-safety issues in the Senior School.

The DSLs work with the Bursar and Network Manager to review both the strategic and practical management of e-safety in Bradford Grammar School (the "School") on a continuing basis. This includes providing specific education for pupils regarding e-safety as part of the Personal Development Programme and making all employees aware of the safeguarding issues associated with the use of technology.

The DSLs will keep a record of any safeguarding issues related to the misuse of IT which forms part of the annual safeguarding report presented to Governors.

In essence, the guiding tenets of the School's Child Protection Policy are also followed with respect to e-safety, namely:

- *Prevention* - through the promotion of a positive School atmosphere and the provision of careful and vigilant teaching and pastoral support;
- *Protection* - by following agreed procedures and ensuring that all employees are appropriately recruited and then trained and supported to respond sensitively to child protection concerns; and
- *Support* - for all those pupils who may have been abused.

This policy applies to all employees and volunteers working in the School as well as the Governors. The School recognises that high self-esteem, confidence, supportive friends and clear lines of communication with a trusted adult will help to protect pupils against potential abuse.

The School will therefore:

- continue to maintain an ethos in which young people feel secure and know that their concerns will be taken seriously;
- ensure that the pupils know that there are adults in School who can be approached if they are worried or are in any kind of difficulty; and
- include within the Personal Development Programme sessions that help pupils to gain an awareness of the issues involved; promote their own safety; and help them to understand the responsibilities of adult life, particularly with regard to the care of children.

2. Practice

The Network Manager has responsibility for ensuring that the School's technical infrastructure is secure and not open to misuse or malicious attack. Access to the School network and devices is protected in accordance with the Data Protection Policy which is reviewed regularly.

With this in mind, the Network Manager is required to keep up-to-date with technical e-safety information in order to effectively carry out the e-safety role and to inform and advise the DSLs and SLT as appropriate.

Through regular training, and updating and delivery of the Personal Development Programme, the DSLs will keep abreast of current issues and the latest advice relating to safeguarding and the use of IT by young people.

Teaching and non-teaching employees are responsible for ensuring that they are aware of e-safety matters and the current School E-Safety Policy. Employees must also sign the School's Acceptable Use Policy and follow the Code of Safe Practice.

Employees must report any suspected misuse of IT by a pupil or employee to a member of SLT. Safeguarding issues associated with the misuse of IT should be brought to the attention of one of the DSLs in accordance with the Child Protection Policy.

Pupils are responsible for using IT in School in accordance with the Pupil's Acceptable Use Policy. The safe use of IT forms part of the Personal Development Programme in which pupils gain an understanding of, for example, the issues surrounding social media, the use of digital imagery, data security and cyber-bullying.

It is accepted that, on occasion, pupils may need to research topics that would normally result in internet searches being blocked. In such circumstances, employees can request that these sites be temporarily unblocked, but requests of this nature must first be sanctioned by the Pastoral or Academic Director.

Parents play an important role in ensuring that their children recognise the need to use the internet and social media responsibly and the School will provide opportunities for parents to understand these issues through evening presentations, InTouch communications, newsletters and information on the School's website.

2. Inappropriate activities - pupils

Some internet activity, for example accessing child pornography or distributing racist material, is illegal and is banned from the School system. The police will always be informed if there is a suspicion that the School's IT infrastructure has been used illegally.

Other activities like cyber-bullying are also banned and could lead to criminal prosecution.

Other, legal, activities may be considered to be inappropriate in a School context due to the age of the pupils or the specific nature of the activities and these may also be subject to restriction.

In the event of suspicion that a pupil has used the School's IT infrastructure inappropriately, or has used the internet and/or social media in such fashion that it may cause harm to the School, employees or pupils, an investigation will be led by the Pastoral Director. It is likely that any investigation will also involve other members of SLT, Heads of Year and the Network Manager. The School's Behaviour Policy contains details of the potential sanctions that may be applied.

In cases where there is safeguarding issue, the DSLs (of which the Pastoral Director is one) may make a referral to Bradford Children's Services or CAMHS as appropriate. However, any adult can make a referral should they have a legitimate safeguarding concern (see Child

Projection Policy).

3. Inappropriate activities – employees

In the event of suspicion that an employee has used the School IT infrastructure appropriately, or has used the internet and/or social media in such fashion that it may cause harm to the School, employees or pupils, an investigation will be led by the Deputy Head or Bursar as appropriate, supported by employees from the Human Resources Department.

Minor or major breaches of School policy may result in disciplinary action being undertaken.

Any potential safeguarding concern must be brought to the attention of the DSLs, of which the Deputy Head is one, and appropriate action will be undertaken (see Child Protection Policy).

If the nature of the activity is illegal, a referral to the local police will be made immediately.

Such activity includes:

- viewing, downloading and/or distributing images of child abuse;
- incidents of 'grooming' behaviour;
- sending obscene materials to a child;
- viewing, downloading and/or distributing adult materials which potentially breach the Obscene Publications Act;
- viewing, downloading and/or distributing criminally racist material; and
- other criminal conduct.

In this situation, it may be necessary to isolate a School computer or other School IT infrastructure pending a police enquiry.