

## **LAMBOURNE END E-SAFETY POLICY**

### **SCOPE**

This policy provides guidance on the procedures that will support and underpin the use of and access to computers, the internet, social networking and other online services within Lambourne End Centre.

This e-safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use at Lambourne End Centre.

This policy should be read in conjunction with the:

- Safeguarding Policy
- Anti-bullying Policy
- Information and Communication Technology Policy

### **STATEMENT OF INTENT**

Lambourne End Limited is committed to safeguarding and protecting the children, young people, vulnerable adults, volunteers and staff of Lambourne End Centre. As such, it is important that all staff, volunteers, Trustees, visitors and anyone working on behalf of the organisation is aware of this e-safety policy and agree to the terms.

### **MAIN AREAS OF RISK**

The main areas of risk associated with using the internet can be summarised as follows:

#### **CONTENT**

- exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with unacceptable language), substance abuse
- lifestyle websites, for example pro-anorexia/self-harm/suicide sites
- hate sites
- content validation: how to check authenticity and accuracy of online content

#### **CONTACT**

- grooming
- cyber-bullying in all forms
- identity theft (including 'frape' (hacking Facebook profiles)) and sharing passwords

#### **CONDUCT**

- privacy issues, including disclosure of personal information
- digital footprint and online reputation
- health and well-being (amount of time spent online (internet or gaming))
- sexting (sending and receiving of personally intimate images) also referred to as SGII (self generated indecent images)
- copyright (little care or consideration for intellectual property and ownership – such as music and film)

## LAMBOURNE END E-SAFETY POLICY

### RESPONSIBILITIES

Lambourne End Limited will ensure that:

- the Centre uses an approved, filtered Internet Service with a password protected WIFI connection.
- all computers and laptops are password protected.
- All staff and volunteers receive the appropriate training with regards to e-safety.

All staff and volunteers must:

- understand and agree to the Information and Communications Policy.
- be responsible for using the Centre's ICT systems in accordance with this policy and to model safe, responsible and professional behaviours in their own use of technology.
- ensure that any digital communications with pupils should be on a professional level and only through the Centre's email system or mobile phone, never through personal mechanisms, e.g. personal email, text, mobile phones, social media etc.
- supervise and guide children, young people and vulnerable adults carefully when engaged in learning activities involving online technology.
- be aware of e-safety issues related to the use of mobile phones, cameras and hand held devices such as the distribution of someone's image without their consent.
- assist colleagues working with children, young people or vulnerable adults to work safely and responsibly with the internet and other communication technologies.
- where groups or individuals are required to use the internet for educational purposes, set clear expectations relevant to responsible use. These are communicated to students via the 'Participant Handbook' and 'Student Friendly Code of Conduct'.
- minimise the risk of misplaced or malicious allegations made against adults who work with children, young people or vulnerable adults.
- report any suspected misuse or problem to the Designated Safeguarding Officer
- have clear structures to deal with online abuse such as cyber-bullying, see Anti-bullying Policy.

Lambourne End Limited will ensure that all members of the Centre are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.

All visitors must:

- read, understand and adhere to the Information and Communication Policy
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- understand the importance of reporting abuse, misuse or access to inappropriate materials
- report any suspected misuse or problem to their liaising member of staff or directly to the Safeguarding Officer

The Designated Safeguarding Officer takes overall responsibility for e-safety provision, data and data security. The Officer should be trained in e-safety issues and be aware of the potential for serious 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.

## LAMBOURNE END E-SAFETY POLICY

### HANDLING COMPLAINTS

Lambourne End Limited will take all reasonable precautions to ensure e-safety. However, linked nature of internet content, the international scale and the availability of mobile phones makes it impossible to guarantee that unsuitable material will never appear on a centre computer or mobile device.

The centre cannot accept liability for material accessed or any consequences of internet access.

Staff, volunteers and the children, young people and vulnerable adults are made aware of the infringements in place during their induction. Possible sanctions include:

- interview/counselling by Chief Executive Officer/Safeguarding Officer
- informing parents or carers
- removal of Internet or computer access for a period, [which could ultimately prevent access to files held on the system, including examination coursework]
- referral to LA / Police.

The Designated Safeguarding Officer acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Chief Executive. See Complaints and Whistleblowing Policy.

Complaints of cyber-bullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with the Safeguarding Policy.

Signed:



Date: 12/09/23

Position: CEO